PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-272695
(43)Date of publication of application : 18.10.1996

(51)Int.Cl. G06F 12/14
G06F 1/00

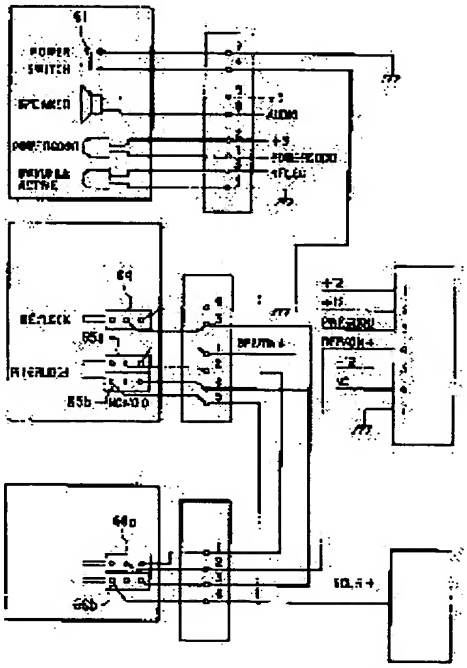
(21)Application number : 08-015533
(22)Date of filing : 31.01.1996

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : DAYAN RICHARD A
NEWMAN PALMER E

(30)Priority
Priority number : 95 383828 Priority date : 06.02.1995 Priority country : US

(54) SECURITY MANAGEMENT METHOD AND DEVICE IN PERSONAL COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a personal computer system which has a security mechanism that can control an access to data kept in the system.
SOLUTION: This system has a usually closed enclosure, at least one erasable memory element which is selectively activated in an active or inactive states and receives and stores a privilege access password in the active state, an option switch which is ready connected to the erasable memory element and sets the element to an active or inactive states, an illegal access detection switch which is ready connected to the element and detects release of the enclosure and a system processor that is ready connected to the element and controls an access to data on a specified level which is stored in the system by discriminating an input from non input of the stored privilege access password.



LEGAL STATUS

[Date of request for examination]	10.11.1997
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3074641
[Date of registration]	09.06.2000
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平8－272695

(43)公開日　平成８年(1996)10月18日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｃ	
				３２０Ｄ	
1/00	３７０		1/00	３７０Ｅ	

審査請求　未請求　請求項の数22　ＯＬ　外国語出願　（全 95 頁）

(21)出願番号　特願平8－15533

(22)出願日　平成８年(1996)１月31日

(31)優先権主張番号　３８３８２８

(32)優先日　1995年２月６日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　リチャード・エイ・ダイアン
アメリカ合衆国フロリダ州ボカ・ラトン、ノース・イースト、セブンティー・サード・ストリート830番地

(74)代理人　弁理士　合田　潔　（外２名）

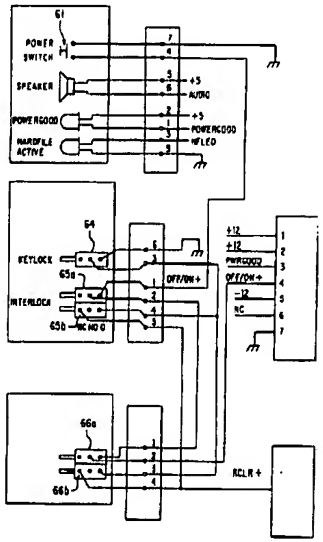
最終頁に続く

(54)【発明の名称】　パーソナル・コンピュータにおけるセキュリティ管理方法及び装置

(57)【要約】

【課題】　システム内に保持されているデータへのアクセスの制御を可能にするセキュリティ機構を有するパーソナル・コンピュータ・システムを提供する。

【解決手段】　このシステムは、常時閉じられたエンクロージャと、活動状態と非活動状態に選択的に活動化され活動状態のときに特権アクセス・パスワードを受け取って記憶する少なくとも１つの消去可能メモリ素子と、消去可能メモリ素子に作動可能に接続され、消去可能メモリ素子を活動状態および非活動状態に設定するオプション・スイッチと、消去可能メモリ素子に作動可能に接続され、エンクロージャの開放を検出する不正アクセス検出スイッチと、消去可能メモリ素子に作動可能に接続され、記憶されている特権アクセス・パスワードの入力と非入力を区別することによってシステム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを有する。



【特許請求の範囲】

【請求項１】データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、

常時閉じられているエンクロージャと、

前記エンクロージャ内に実装され、活動状態と非活動状態への選択的活動化を行い、活動状態のときに特権アクセス・パスワードを受け取って記憶する消去可能メモリ素子と、

前記消去可能メモリ素子に作動可能に接続され、前記消去可能メモリ素子を活動状態および非活動状態に設定するためにパーソナル・コンピュータ・システムのユーザによって手動設定可能な、前記エンクロージャ内に実装された手動操作可能なオプション・スイッチと、

移動検出スイッチと、

移動検出スイッチを選択的にイネーブルおよびディスエーブルする手段と、

前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する前記移動検出スイッチと、移動検出スイッチを含み、前記移動検出スイッチがイネーブルされているときに前記移動検出スイッチの任意の切換えに応答して、コンピュータ・システムの電力投入の成功を妨げる手段と、

前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、パスワードの入力と非入力および移動検出スイッチのイネーブル状態とディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含むシステム。

【請求項２】システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化することを特徴とする、請求項１に記載のパーソナル・コンピュータ・システム。

【請求項３】消去可能メモリ素子が電源投入パスワードを受け取って記憶し、前記システム・プロセッサが移動検出スイッチの切換え後の電源投入中に、システムのユーザが電源投入パスワードの入力に成功するとシステムを活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにすることを特徴とする、請求項１に記載のパーソナル・コンピュータ・システム。

【請求項４】前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、請求項３に記載のパーソナル・コンピュータ・システム。

【請求項５】システム・プロセッサが、消去可能メモリ素子内のいずれかのパスワードの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、請求項４に記載のパーソナル・コンピュータ・システム。

【請求項６】システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対して移動検出スイッチの切換えの標識を提供することを特徴とする、請求項１に記載のパーソナル・コンピュータ・システム。

【請求項７】移動検出スイッチが、エンクロージャ内の水平面に取り付けられた２対の水銀リード・スイッチを含み、１対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該２対の水銀リードスイッチの傾斜によって少なくとも１つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、請求項１に記載のパーソナル・コンピュータ・システム。

【請求項８】データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、

常時閉じられているエンクロージャと、

前記エンクロージャ内に実装され、活動状態と非活動状態への選択的活動化を行い、活動状態のときに電源投入パスワードと特権アクセス・パスワードを受け取って記憶する消去可能メモリ素子と、

前記消去可能メモリ素子に作動可能に接続され、前記消去可能メモリ素子を活動状態および非活動状態に設定するためにパーソナル・コンピュータ・システムのユーザによって手動設定可能な、前記エンクロージャ内に実装された手動操作可能なオプション・スイッチと、

前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されて前記エンクロージャの開放を検出する不正アクセス検出スイッチと、

前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する移動検出スイッチと、

移動検出スイッチを選択的にイネーブルおよびディスエーブルするプログラム被制御手段と、

不正アクセス検出スイッチまたは前記移動検出スイッチがイネーブルされているときに不正アクセス検出スイッチまたは前記移動検出スイッチの切換えに応答して、コンピュータ・システムの電源投入の成功を妨げる手段と、

前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、前記メモリ素子の活動状態と非活動状態、パスワードの入力と非入力、および移

動検出スイッチのイネーブルとディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含む、パーソナル・コンピュータ・システム。

【請求項９】前記システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにすることを特徴とする、請求項８に記載のパーソナル・コンピュータ・システム。

【請求項１０】前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、請求項９に記載のパーソナル・コンピュータ・システム。

【請求項１１】システム・プロセッサが、システムのユーザによるパスワードの１つの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、請求項１０に記載のパーソナル・コンピュータ・システム。

【請求項１２】システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対して移動検出スイッチの切換えの標識を提供することを特徴とする、請求項８に記載のパーソナル・コンピュータ・システム。

【請求項１３】移動検出スイッチが、エンクロージャ内の水平面に取り付けられた２対の水銀リード・スイッチを含み、１対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該２対の水銀リードスイッチの傾斜によって少なくとも１つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、請求項８に記載のパーソナル・コンピュータ・システム。

【請求項１４】データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、

常時閉じられているエンクロージャと、

移動検出スイッチと、

移動検出スイッチを選択的にイネーブルおよびディスエーブルするプログラム制御手段と、

前記エンクロージャ内に実装され、活動状態と非活動状態に選択的に活動化され、活動状態のときに特権アクセス・パスワードを受け取って記憶する第１の消去可能メモリ素子と、

前記エンクロージャ内に取り付けられ、前記第１の消去可能メモリ素子に作動可能に接続されて、前記第１の消去可能メモリ素子を活動状態および非活動状態に設定するオプション・スイッチと、

前記エンクロージャ内に実装され、電源投入パスワードおよび、移動検出スイッチのイネーブル状態と、第１の消去可能メモリ素子の状態と、記憶されている任意の電源投入パスワードおよび特権アクセス・パスワードの正しいインストールとを示すデータを受け取って記憶する第２の消去可能メモリ素子と、

前記エンクロージャ内に取り付けられ、前記第２の消去可能メモリ素子に作動可能に接続されて前記エンクロージャの無許可の開放を検出する不正アクセス検出スイッチと、

前記エンクロージャ内に取り付けられ、前記第２の消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する前記移動検出スイッチと、

特権アクセス・パスワードがインストールされている状態で効力を生じ、不正アクセス検出スイッチの切り換えに応答し、移動検出スイッチがイネーブルになっているときに移動検出スイッチの切り換えに応答して、コンピュータ・システムの電源投入の成功を妨げる手段と、

前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、移動検出スイッチのイネーブル状態とディスエーブル状態、および第１および第２の消去可能メモリ素子内の記憶されている任意の有効な特権アクセス・パスワードおよび記憶されている任意の有効な電源投入パスワードの入力と非入力を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含む、パーソナル・コンピュータ・システム。

【請求項１５】前記システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにすることを特徴とする、請求項１４に記載のパーソナル・コンピュータ・システム。

【請求項１６】前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、請求項１５に記載のパーソナル・コンピュータ・システム。

【請求項１７】システム・プロセッサが、システムのユーザによるパスワードの１つの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、請

求項１６に記載のパーソナル・コンピュータ・システム。

【請求項１８】システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対してイネーブルされている移動検出スイッチの切換えの標識を提供することを特徴とする、請求項１５に記載のパーソナル・コンピュータ・システム。

【請求項１９】移動検出スイッチが、エンクロージャ内の水平面に取り付けられた２対の水銀リード・スイッチを含み、１対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該２対の水銀リードスイッチの傾斜によって少なくとも１つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、請求項１４に記載のパーソナル・コンピュータ・システム。

【請求項２０】エンクロージャと、エンクロージャ内に実装されたシステム・プロセッサと、エンクロージャ内に実装された選択的活動化が可能な消去可能メモリ素子と、エンクロージャ内に装着されてパーソナル・コンピュータ・システムのユーザが手動で設定することができる、メモリ素子を活動状態および非活動状態に設定する手動操作可能オプション・スイッチと、エンクロージャ内に装着され、エンクロージャの開放を検出する不正アクセス検出スイッチと、エンクロージャ内に装着され、コンピュータ・システムの平常稼働位置からの移動を検出する移動検出スイッチと、移動検出スイッチをイネーブル状態にするユーザ呼出し可能ユーティリティ・プログラムとを有するパーソナル・コンピュータ・システムを操作する方法であって、

オプション・スイッチを手動で設定し、メモリ素子を活動状態に選択的に設定するステップと、

活動メモリ素子に特権アクセス・パスワードを記憶するステップと、

移動検出スイッチをイネーブルするユーティリティ・プログラムを呼び出すステップと、

パスワードの入力と非入力および移動検出スイッチのイネーブル状態とディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するステップと、

不正アクセス検出スイッチの任意の切り換えに応答し、イネーブルされている移動検出スイッチの切換えに応答して、システムの電源投入を妨げるステップとを含む方法。

【請求項２１】メモリ素子に電源投入パスワードを記憶するステップと、

移動検出スイッチの切り換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力の成功に応答してシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにするステップとをさらに含むことを特徴とする、請求項２０に記載の方法。

【請求項２２】電源投入パスワード入力の試行の失敗の後に、システムのユーザによる特権アクセス・パスワードの入力の成功に応答してシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにするステップをさらに含む、請求項２０に記載の方法。

【発明の詳細な説明】

【０００１】本明細書で記述する本発明は、１９９２年２月２６日出願の「Personal Computer System With Security Features and Method」という名称の米国特許出願第８４０９６５号に記述されている発明および１９９２年５月２２日出願の「Trusted Personal Computer System With Limited Accessibility」という名称の米国特許出願第０７／８８９３２５号で記述されている発明に関連し、両者は本出願と共通の出願人に帰する。

【０００２】

【発明の属する技術分野】本発明は、パーソナル・コンピュータ・システムに関し、具体的にはシステムで保持されているデータへのアクセスの制御を可能にするセキュリティ機構を有するシステムに係わる。

【０００３】

【従来の技術】一般にパーソナル・コンピュータ、具体的にはＩＢＭパーソナル・コンピュータは、今日の近代化社会の多くの部門にコンピュータ機能を提供するために広く利用されている。パーソナル・コンピュータ・システムとは通常、単一のシステム・プロセッサとそれに関連する揮発性メモリおよび不揮発性メモリを有するシステム装置、表示モニタ、キーボード、１つまたは複数のディスケット・ドライブ、固定ディスク記憶装置、および任意選択の印刷装置で構成されている、デスクトップ、床置き型、または携帯型マイクロコンピュータと定義することができる。これらのシステムを他と区別する特徴の１つは、マザーボード（本明細書ではシステム・ボード、システム・プレーナと呼ぶ場合もある）を使用してこれらの構成機器すべてを電気的に接続することである。このようなシステムは、主として単一ユーザに独立したコンピュータ機能を提供するように設計され、個人または小企業が購入するのに手頃な価格となっている。このようなパーソナル・コンピュータ・システムの例は、ＩＢＭのパーソナル・コンピュータＡＴおよびＩＢＭのパーソナル・システム／２のモデル２５、３０、３５、４０、Ｌ４０ＳＸ、５０、５５、５７、６５、７０、８０、９０、および９５である。

【０００４】これらのシステムは大きく２つのファミリに分類することができる。第１のファミリは、通常、ファミリＩモデルと呼ばれ、ＩＢＭパーソナル・コンピュータＡＴおよびその他の「ＩＢＭ互換」機によって代表されるバス・アーキテクチャを使用している。第２のフ

ファミリは、ファミリＩＩモデルと呼ばれ、ＩＢＭのパーソナル・システム／２のモデル５０ないし９５によって代表されるマイクロ・チャネル・バス・アーキテクチャを使用している。初期のファミリＩモデルは一般に、普及していたインテル８０８８または８０８６マイクロプロセッサをシステム・プロセッサとして使用していた。最近の一部のファミリＩと、ファミリＩＩモデルは一般に、より低速のインテル８０８６マイクロプロセッサをエミュレートするリアル・モードか、または一部のモデルの場合にアドレス範囲を１メガバイトから４ギガバイトに拡張するプロテクト・モードで動作することができる高速のインテル８０２８６、８０３８６、および８０４８６マイクロプロセッサを使用している。本質的には、８０２８６、８０３８６および８０４８６プロセッサのリアル・モード機能は、８０８６および８０８８マイクロプロセッサ用に作成されたソフトウェアとのハードウェア互換性を備える。

【０００５】近年の世界におけるパーソナル・コンピュータの驚異的な増大と使用に伴って、ますます多くのデータまたは情報が収集され、このようなシステムに保持または記憶されるようになっている。このデータの多くは機密的性質のものである。データは不正な人の手に渡ると個人にとって不都合なことになる恐れがあり、会社は競争優位を失うことがある。あるいは、機密データが口止め料の強要に利用されたり、個人に対する人身暴力に至る恐れがある。データの機密的性質と価値を認識するユーザが増えるに従って、このような悪用から保護することがますます望まれるようになる。ユーザ自身と記憶されているデータの関係者とを保護するために、ユーザは、購入するパーソナル・コンピュータにセキュリティ機構と保全性機構を組み込むことが必要になりつつある。

【０００６】収集され記憶されるデータの機密性を認識しているのはユーザだけにとどまらない。各国政府も、機密データの保護を実施する法律を制定しようとしている。そのような政府の１つは米国政府である。米国政府は、状況の重大さを認識し、対処している。米国連邦政府は、セキュリティ・レベルと、それらのレベルを満たすために必要な関連要件を規定しており、製品が製造業者の主張するセキュリティ・レベルを満たしているかどうかを調べるために、パーソナル・コンピュータ製造業者が製品を提出するための認証政府機関を設けている。この連邦要件の拠り所は、一般に「オレンジ・ブック」と呼ばれている「Department of Defense, Trusted Computer System Evaluation Criteria（国防総省トラステッド・コンピュータ・システム評価基準）DOD ５２００．２８STD，１２／８５」である。米国政府は、１９９２年１月１日まで政府に関係するデータはすべて、Ｃ－２の最低セキュリティ・レベルを有するパーソナル・コンピュータでのみ処理し、記憶しなければならないと定めている。コンピュータ・システムのハードウェアについては、この要件の要綱は保証節の要件６「トラステッド機構は不正アクセスまたは無許可の変更あるいはその両方から絶えず保護されなければならない．．．」という箇所に記載されている。

【０００７】ＩＢＭパーソナル・コンピュータなどのファミリＩモデルの最も初期のパーソナル・コンピュータ・システム以来、ソフトウェア互換性が最も重要となると認識されていた。この目標を達成するために、ハードウェアとソフトウェアの間に「ファームウェア」とも呼ばれるシステム常駐コードの隔離層が設定された。このファームウェアは、ユーザのアプリケーション・プログラム／オペレーティング・システムと装置の間に操作インタフェースを設けて、ユーザがハードウェア装置の特性について気にしなくても済むようにした。最終的に、このコードは基本入出力システム（ＢＩＯＳ）に発展し、システムに新しい装置を追加することができるようにすると同時に、アプリケーション・プログラムをハードウェアの特性から隔離している。ＢＩＯＳはデバイス・ドライバを特定の装置ハードウェア特性への依存から解放したと同時に、デバイス・ドライバに装置への中間インタフェースを提供したため、ＢＩＯＳの重要性はただちに明らかになった。ＢＩＯＳはシステムに組み込まれた部分であり、システム・プロセッサに入出力されるデータの動きを制御したため、システム・プレーナ上に常駐し、ユーザに対しては読み取り専用メモリ（ＲＯＭ）で出荷された。たとえば、最初のＩＢＭパーソナル・コンピュータのＢＩＯＳは、プレーナ・ボード上の８ＫバイトのＲＯＭを占有した。

【０００８】このパーソナル・コンピュータ・ファミリの新しいモデルが導入されるに従って、新しいハードウェアおよび入出力装置を組み込むようにＢＩＯＳを最新化し、拡張しなければならなかった。予想されたように、ＢＩＯＳはメモリ・サイズを増大させ始めた。たとえば、ＩＢＭパーソナル・コンピュータＡＴの導入に伴って、ＢＩＯＳは３２KバイトのＲＯＭを必要とするまでになった。

【０００９】今日、新技術の発達に伴って、ファミリＩＩモデルのパーソナル・コンピュータ・システムはますます高度化しており、消費者は一層頻繁に利用することができるようになっている。技術が急速に変化し、パーソナル・コンピュータ・システムに新しい入出力装置が追加されるため、パーソナル・コンピュータ・システムの開発サイクルにおいてはＢＩＯＳの修正が重要な問題になっている。

【００１０】たとえば、マイクロ・チャネル・アーキテクチャを有するＩＢＭパーソナル・システム／２の導入に伴って、拡張ＢＩＯＳまたはＡＢＩＯＳと呼ばれるきわめて新しいＢＩＯＳが開発された。しかし、ソフトウェア互換性を維持するため、このファミリＩＩモデルにファミリＩモデルのＢＩＯＳを組み込まなければならなかった。ファミリＩのＢＩＯＳは互換性ＢＩＯＳまたはＣＢＩＯＳと呼ばれるようになった。しかし、前記でＩＢＭパーソナル・コンピュータＡＴに関して述べたように、プレーナ・ボードには３２KバイトのROMしか搭載されていなかった。幸いにも、このシステムはROMを９６Kバイトに拡張することができた。しかし残念ながら、システムの制約のため、これはＢＩＯＳの最大使用可能容量であることがわかった。幸運なことに、ＡＢＩＯＳを追加しても、ＡＢＩＯＳとＣＢＩＯＳを９６KのROMに押し込むことができた。しかし、９６KのROM領域には拡張のために使用可能な領域はわずかな割合しか残っていない。将来、入出力装置を追加すると、ＣＢＩＯＳとＡＢＩＯＳは最終的にROMスペースを使い果たしてしまうことになる。したがって、ＣＢＩＯＳとＡＢＩＯＳ内に新しい入出力技術を組み込むことは容易にはできないであろう。

【００１１】上記の問題のほか、開発サイクルのできるだけ遅い時点でファミリＩＩ　ＢＩＯＳに修正を加えたいために、ROMからＢＩＯＳの一部をオフロードすることが必要になった。これは、ＢＩＯＳの一部を、固定ディスクなどの大容量記憶装置、好ましくはそのようなディスクのシステム区画と呼ばれる画定された部分に、記憶することによって実現された。このシステム区画には、システム構成などの設定に使用される特定のユーティリティ・プログラムが入っているシステム・リファレンス・ディスケットのイメージも記憶される。ディスクは読み取り機能だけでなく書込み機能も備えるため、ディスク上の実際のＢＩＯＳコードを修正することが可能になった。ディスクは、ＢＩＯＳコードを記憶する速くて効率的な方法を提供するが、それにもかかわらず、ＢＩＯＳコードが破壊される確率を大幅に増大させた。ＢＩＯＳはオペレーティング・システムの組込み部分であるため、ＢＩＯＳが破壊されると、徹底的に損害を受ける結果となることがあり、システムの全面的障害となり動作不能になる場合が多い。したがって、固定ディスク上のＢＩＯＳの無許可の修正を防止する手段が強く望まれることが明確に明らかになった。これは、１９８９年８月２５日出願の米国特許出願第０７／３９８８２０号、現在は１９９１年６月４日発行の米国特許第５０２２０７７号となっている特許の主題であった。関心があれば、本明細書で開示されている発明の理解の助けとなる可能性のある付加的情報について、上記の特許を参照されたい。上記特許の開示は、本明細書で開示されている発明を十分に理解するのに必要な程度まで参照により本明細書に組み込まれる。

【００１２】ＩＢＭのＰＳ／２マイクロ・チャネル・システムの導入に伴って、入出力アダプタ・カードおよびプレーナからスイッチとジャンパが除去された。それらに代わって、プログラマブル・レジスタのためのマイクロ・チャネル・アーキテクチャが備えられた。これらのプログラマブル・レジスタまたはプログラマブル・オプション・セレクト（ＰＯＳ）レジスタを構成するためのユーティリティが必要であった。各システムは、これらのユーティリティと、システムの可用性特性およびシステム診断機能を向上させるためのその他のユーティリティが入ったシステム・リファレンス・ディスク付きで出荷された。

【００１３】初期使用の前に、各マイクロ・チャネル・システムはそのＰＯＳレジスタの初期設定を必要とした。たとえば、新しい入出力カードを使用するかまたは入出力カードのスロット変更を行ってシステムをブートした場合、構成エラーが発生し、システム・ブート・アップ手続きが停止する。その場合、ユーザにはシステム・リファレンス・ディスケットをロードしてＦ１キーを押すようにプロンプトが出される。すると、システム・リファレンス・ディスケットから「Set Configuration Utility（構成設定ユーティリティ）」をブートすることができる。「構成設定ユーティリティ」によって、ユーザは所望のアクションを行うように求められる。適切な入出力カードのディスクリプタ・ファイルがシステム・リファレンス・ディスケット上にロードされている場合、「構成設定ユーティリティ」は不揮発性記憶装置で適切なＰＯＳまたは構成データを生成する。ディスクリプタ・ファイルには、カードをシステムとインタフェースさせるための構成情報が入っている。

【００１４】関連出願番号第８４０９６５号では、特定の重要データへのアクセスを、前記データにアクセスする適正な権限を有するユーザにのみ制限する手段を備えるパーソナル・コンピュータについて述べられている。この目的を実現するために、「電源投入パスワード」と「特権アクセス・パスワード」（以下、それぞれ「ＰＯＰ」および「ＰＡＰ」と呼ぶ場合がある）を受け取り記憶するためと、様々な機能およびデータへの許可されるアクセスをパスワードの活動化と使用に合わせて調整するための、専用メモリ素子が備えられている。ユーザは、提供されたセキュリティ条件を活動化するか非活動化するかを選択することができ、システムの使用を安全保護する必要や希望の変化にシステムを合わせることができるようになっている。システムは、所望であれば政府規格のセキュリティ要件に適合させることができ、さらに、状況が許す場合には本質的に安全保護されていない形で使用することもできる。したがって、このようなシステムのユーザは、システムの使用において高い柔軟性を得ることができる。この関連出願の教示については、以下で、本出願の発明との関連に鑑みて詳述する。

【００１５】

【発明が解決しようとする課題】上記に鑑みて、本発明は、物理的ハードウェアを盗難から保護するのではなく、従来の技術で開示されている他のセキュリティ機構

と組み合わせたとき、パーソナル・コンピュータに記憶されているデータを役に立たなくすること、すなわち、無許可のユーザがアクセスできなくすることに重きを置いた、新しいパーソナル・コンピュータ機構を企図している。

【課題を解決するための手段】

【００１６】この新しいセキュリティ機構は、パーソナル・コンピュータ・システムを通常の稼働位置から移動させた場合、その後、パーソナル・コンピュータ・システムを無許可のユーザ、すなわちシステム・パスワードを知らない人が操作することができなくする。したがって、万一システムが盗まれた場合、無許可のユーザは、システム構成要素内に入っている少なくとも特定の指定データにアクセスすることができない。

【００１７】本発明の好ましい実施例では、前記で述べ、以下で詳述するタイプのパーソナル・コンピュータ・システムは、平常位置合わせされている稼働位置からのシステムの移動を検出する任意選択機能を備えていることが好ましい。そのような移動を検出すると、移動検出装置が前述の従来の技術の不正アクセス明示機構またはそれを変更した機構を作動させる。その後、システムは、システムの所有者、許可されたユーザ、または通常のユーザが、電源を遮断した後、電源投入ルーチン時にパスワードを求めるプロンプトに応答してＰＯＰまたはＰＡＰあるいはその両方を入力することによってのみ起動することができる。

【００１８】

【発明の実施の形態】上記の本発明のいくつかの目的およびその他の目的は、添付図面を参照しながら説明を進めるうちに明らかになろう。

【００１９】以下では、本発明について、本発明の好ましい実施例が図示されている添付図面を参照しながら詳細に説明するが、以下の説明の始めに、当業者なら本明細書に記載されている本発明に変更を加えて本発明の好都合な結果を得ることができることを理解されたい。したがって、以下の説明は当業者を対象とする概略的、教示的な開示であって、本発明を限定するものではないものと理解されたい。

【００２０】本明細書では、以下のように、特定の定義された用語を使用することがある。

トラステッド・コンピューティング・ベース（ＴＣＢ）：その組合せによってセキュリティ方針が実施されるハードウェア、ファームウェア、およびソフトウェアを含むコンピュータ・システム内の保護機構の全体。ＴＣＢは、全体としてある製品またはシステムに対する統一したセキュリティ方針を実施する、１つまたは複数の構成要素からなる。ＴＣＢがセキュリティ方針を正しく実施できるかどうかは、ＴＣＢ内の機構と、セキュリティ方針に関係するパラメータ（たとえばユーザのクリアランス）をシステム管理者が正しく入力するかどうかにかかっている。

トラステッド・ソフトウェア：「トラステッド・コンピューティング・ベース」のソフトウェア部分。「トラステッド・コンピューティング・ベース」上で動作可能なプログラムであって、「トラステッド・プログラム」以外のプログラム。

参照監視概念（reference monitor concept）：主体による客体へのすべてのアクセスを仲介する抽象計算機を指すアクセス制御概念。

セキュリティ・カーネル：参照監視概念を実現する「トラステッド・コンピューティング・ベース」のハードウェア、ファームウェア、およびソフトウェア要素。すべてのアクセスを仲介しなければならず、変更から保護され、正しいことが検証されなければならない。

トラステッド・コンピュータ・システム：ある範囲の機密情報または秘密情報を同時に処理するために使用することができる十分なハードウェアおよびソフトウェア保全性を採用するシステム。

システム所有者：システム所有者は、最初にシステムを構成して安全保護モードにする責任を負う人である。システム所有者は、初期および更新によって必要になったときに、構成を管理する。システム所有者は、「特権アクセス・パスワード」を管理するとともに、その保全性を維持する責任を負う。システム所有者は不正アクセス明示カバー・キーロック・キーの物理的セキュリティも維持する。システム所有者は、すべてのシステム上のセキュリティ・ログを維持する責任を負う。システム所有者は、セキュリティ侵害の試行もすべて記録しなければならない。システム所有者は複数のシステムを所有することもできる。システム所有者は、許可ユーザとみなされ、通常ユーザともなることができる。

安全保護モード（secure mode）：システム所有者がパーソナル・コンピュータ・システムに「特権アクセス・パスワード」のインストールに成功すると、セキュリティ要素と保全性要素によってセキュリティ保護が設けられる。

許可ユーザ：「特権アクセス・パスワード」の使用許可が与えられているすべてのユーザである。このユーザはシステム所有者であるかどうかを問わない。このユーザは、特定の１台のシステムまたは１組のシステムのキーを持つことができる。このユーザがセキュリティ侵害からシステムを回復させることに関与する場合は、それをシステム所有者に報告する責任がある。許可ユーザは通常ユーザであることもできる。

通常ユーザ：システム機能を使用することを許可されている、システムのあらゆるユーザである。システム構成の変更または問題の修復を行うために、このユーザはシステム所有者または許可ユーザの援助を必要とする。通常ユーザは、特権ユーザまたはシステム所有者のカテゴリに属していない場合、「特権アクセス・パスワード」

または不正アクセス明示カバー・キーロック・キーを持たない。

無許可ユーザ：システム所有者、許可ユーザ、または通常ユーザとして定義されていないあらゆるユーザである。電源投入の失敗を除き、安全保護されたパーソナル・コンピュータ・システムを無許可ユーザが使用した場合はすべて、セキュリティ侵害とみなされ、そのような侵害を示す監査証跡が存在しなければならない。

ＥＥＰＲＯＭ：電気的消去可能プログラマブル読み取り専用メモリ。このメモリ技法によって、ハードウェア論理回路の制御で変更可能なデータの不揮発性記憶を行うことができる。電力供給がないときでも記憶域の内容は失われない。モジュール上で適切な制御信号を所定の順序で活動化したときにのみ、内容を変更することができる。

パスワード記述：システムは、１．特権アクセス・パスワード（ＰＡＰ）と２．電源投入パスワード（ＰＯＰ）の２つのパスワードによって保護することができる。この２つのパスワードは、互いに独立して使用するように意図されている。ＰＡＰは、初期プログラム・ロード（ＩＰＬ）デバイス・ブート・リスト、パスワード・ユーティリティへのアクセス、およびシステム・リファレンス・ディスケットまたはシステム区画へのアクセスを保護することによってシステム所有者を保護する。ＰＡＰがインストールされていないか、または電源投入手順時にＰＡＰを最初に入力した場合、システム区画はＰＯＳＴエラーに応答して（またはウォーム・ブート時）のみブートされる。ディスケットからの初期ＢＩＯＳロード（ＩＢＬ）は、システム・リファレンス・ディスケットのブートと同様にして安全保護される。ＰＡＰの存在は、ＰＯＰを使用する通常ユーザには見えない。ＰＡＰは、システム・リファレンス・ディスケット上またはシステム区画内のユーティリティによってインストール、変更、または削除することができる。ＰＡＰを設定して正しく入力すると、所有者はシステム全体にアクセスすることができるようになり、ＰＯＰが上書きされる。ＰＯＰはすべての現行ＰＳ／２システムで機能し、ＤＡＳＤ上のオペレーティング・システムまたはシステムの機能へのあらゆる無許可のアクセスを防止する。

【００２１】次に、各図面を具体的に参照すると、１０（図１）に本発明を実施するマイクロコンピュータが図示されている。前述のように、コンピュータ１０はそれに付随するモニタ１１、キーボード１２、および印刷装置またはプロッタ１４を有することができる。コンピュータ１０は、図２に示すように、ディジタル・データの処理と記憶を行う、電力供給されるデータ処理構成要素および記憶構成要素を収容する密封遮蔽された空間を、シャーシ１９と共に画定するカバー１５を有する。図２に図示する態様では、コンピュータ１０は、コンピュータ・システムと接続する入出力ケーブルの接続点の上に延び、その接続点を保護する任意選択の入出力ケーブル接続カバー１６も有する。システム構成要素のうちの少なくとも一部は、シャーシ１９に取り付けられて、前記の構成要素およびフロッピィ・ディスク・ドライブ、様々な形態のダイレクト・アクセス記憶装置、アクセサリ・カードまたはボードおよび同様のものなど、関連するその他の要素を含むコンピュータ１０の構成要素を電気的に相互接続する手段を提供する多層プレーナ２０（本明細書ではマザー・ボードまたはシステム・ボードとも呼ぶ）上に実装されている。

【００２２】シャーシ１９は、基部と背面パネルを有し（図２、ケーブル接続カバー１６によって外部から覆うこともできる）、磁気ディスクまたは光ディスクのディスク・ドライブ、テープ・バックアップ・ドライブ、または同様のものなどデータ記憶装置を収容する少なくとも１つのオープン・ベイを画定する。図示されている態様では、上部ベイ２２は第１のサイズの周辺装置ドライブ（３．５インチ・ドライブと呼ばれるドライブなど）を収容するように調整されている。フロッピィ・ディスク・ドライブ、すなわち、その中に挿入されるディスケットを収容することができ、そのディスケットを使用して周知のようにデータの受け取り、記憶、配送を行うことができる取り外し可能媒体ダイレクト・アクセス記憶装置を、この上部ベイ２２に設けることができる。

【００２３】本発明による上記の構造について述べる前に、パーソナル・コンピュータ・システム１０全般の動作を概説する必要がある。図３を参照すると、プレーナ２０上に実装された構成要素および、プレーナと入出力スロットおよびパーソナル・コンピュータ・システムのその他のハードウェアとの接続部を含む、本発明によるシステム１０のようなコンピュータ・システムの様々な構成要素が図示された、パーソナル・コンピュータ・システムのブロック図が示されている。プレーナにはシステム・プロセッサ３２が接続されている。ＣＰＵ３２としては任意の適切なマイクロプロセッサを使用することができるが、１つの好適なマイクロプロセッサはインテルによって販売されている８０３８６である。ＣＰＵ３２は高速ＣＰＵローカル・バス３４によってバス・インタフェース制御ユニット３５、本図ではシングル・インライン・メモリ・モジュール（ＳＩＭＭ）として図示されている揮発性ランダム・アクセス・メモリ（ＲＡＭ）３６、およびＣＰＵ３２への基本入出力操作のための命令が記憶されているＢＩＯＳ　ＲＯＭ３８に接続されている。ＢＩＯＳ　ＲＯＭ３８は、入出力装置とマイクロプロセッサ３２のオペレーティング・システムとをインタフェースさせるために使用されるＢＩＯＳを備えている。ＢＩＯＳ　ＲＯＭ３８に記憶されている命令をＲＡＭ３６にコピーして、ＢＩＯＳの実行時間を短縮することができる。このシステムは、一般的になっているように、バッテリによってバックアップされた不揮発性メモ

リ（従来のCMOS RAM）も有しており、システム構成およびリアル・タイム・クロック（RTC）68に関するデータを受け取って保持するようになっている（図3および図4）。

【0024】以下、本発明について図3のシステム・ブロック図を具体的に参照しながら説明するが、以下の説明の初めに、本発明による装置および方法は、プレーナ・ボードの他のハードウェア構成でも使用可能であるものと理解されたい。たとえば、システム・プロセッサはインテル80286または80486マイクロ・プロセッサとすることもできる。

【0025】図3を参照すると、CPUローカル・バス34（データ、アドレス、および制御構成要素を含む）は、マイクロプロセッサ32と数値演算コプロセッサ39および小型コンピュータ・システム・インタフェース（SCSI）制御装置40との接続も行う。SCSI制御装置40は、コンピュータ設計および運用業者には周知のように、読み取り専用メモリ（ROM）41、RAM42、および図の右側に示されている入出力接続によって容易に接続される適合する様々なタイプの内部装置または外部装置と接続されるか、または接続可能である。SCSI制御装置40は、固定または取り外し可能媒体電磁記憶装置（ハード・ディスク・ドライブおよびフロッピィ・ディスク・ドライブとも呼ぶ）、光磁気、テープ、およびその他の記憶装置などの記憶メモリ装置の制御において、記憶制御装置として機能する。

【0026】バス・インタフェース制御装置（BIC）35が、CPUローカル・バス34を入出力バス44と結合する。BIC35は マイクロ・チャネル・アダプタ・カード45を収容する複数の入出力スロットを有するバス44を使用して、マイクロ・チャネル・バスなどの任意選択の機能バスと結合することができる。マイクロ・チャネル・アダプタ・カード45は、さらに入出力装置またはメモリ（図示せず）に結合することができる。入出力バス44は、アドレス、データ、および制御構成要素を含む。

【0027】入出力バス44には、グラフィック情報の記憶（48に示されている）およびイメージ情報の記憶（49に示されている）を行うビデオRAM（VRAM）と関連するビデオ信号プロセッサ46など様々な入出力構成要素が結合されている。プロセッサ46との間で交換されるビデオ信号は、ディジタル・アナログ変換器（DAC）50を介してモニタまたはその他の表示装置に渡すことができる。VSP46を、ビデオ録画／再生装置、カメラなどの形態をとることができる、本明細書で自然イメージ入出力と呼ぶものに直接接続するための装備もある。入出力バス44にはディジタル信号プロセッサ（DSP）51も接続されており、このDSP51は、DSP51による信号処理のためのソフトウェア命令とそのような処理に関係するデータを記憶するために使用可能な関連する命令RAM52およびデータRAM54を有する。DSP51は、オーディオ制御装置55を備えることによってオーディオ入出力信号を処理することができ、アナログ・インタフェース制御装置56を備えることによってその他の信号を処理することができる。最後に、入出力バス44には、関連する電気的消去可能プログラマブル読み取り専用メモリ（EEPROM）59を有する入出力制御装置58が結合されており、この入出力制御装置58とシリアル・ポートを使用して、フロッピィ・ディスク・ドライブ、印刷装置またはプロッタ14、キーボード12、マウスまたはポインティング・デバイス（図示せず）などの従来の周辺装置との間で入出力データを交換する。

【0028】本明細書で説明するようなパーソナル・コンピュータ・システムを安全保護するという特定の目的を達成するために、パーソナル・コンピュータ・システム10は、システム・エンクロージャ内に、活動状態および非活動状態に選択的に活動化し、活動状態になっているときに特権アクセス・パスワード（以下で詳述する）を受け取って記憶する消去可能メモリ素子を有する。この消去可能メモリ素子は、電気的消去可能プログラマブル読み取り専用メモリ・デバイスすなわちEEPROM59（図3）であることが好ましい。システムには、エンクロージャ内にオプション・スイッチまたはセキュリティ・スイッチが装着されており、消去可能メモリ素子59に作動可能に接続されて、そのメモリ素子を活動状態と非活動状態に設定するようになっている。オプション・スイッチ（本開示ではセキュリティ・スイッチとも呼ぶ）は、たとえばシステム・プレーナ20上に装着されているジャンパとすることができ、プレーナへのアクセス権を有する人が手動で2種類の状態に設定することができる。一方の状態（書込み可能状態とも呼ぶ）では、EEPROM59は活動状態に設定され、本明細書で述べるPAPを記憶する。書込み可能状態ではEEPROMへのPAPの書込み、変更、または除去を行うことができる。他方の状態、すなわち非活動状態では、EEPROMのPAP記憶機能が非活動状態に設定される。

【0029】前述のように、システム10は消去可能メモリ機能を有する第2の構成要素、すなわち、図4の68に示すバッテリ・サポート付きの不揮発性CMOS RAMおよびそれに関連するリアル・タイム・クロック（RTC）も有する。このCMOS RAMには、システム10の電源投入時のPAPの正常な入力に関するデータを含むシステム構成を示すデータが記憶される。少なくとも1つの不正アクセス検出スイッチ（図4、図5、および図6）が、エンクロージャ内に備えられており、CMOS RAMに作動可能に接続されて、不正アクセス検出スイッチの切換えに応答してエンクロージャが開かれたことを検出し、そのメモリ素子に記憶されている特定のデータを消去するようになっている。

【0030】本発明によるシステム・プロセッサ32は、EEPROM59およびCMOS RAM68に作動可能に接続され、メモリ素子のPAP記憶機能の活動状態と非活動状態とを区別し、記憶されている有効な特権アクセス・パスワード（PAP）の入力と非入力とを区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスの制御の一端を担う。システムの操作者（具体的にはセキュリティの監督と維持を担当する人）は、オプション・スイッチを操作して、EEPROMのそれぞれの活動状態と非活動状態を選択することによって、システムの安全保護付き動作と安全保護なし動作とを切り換えることができる。安全保護付き動作を所望し、それを有効にする場合は、システム所有者はPAPを入力しなければならない。

【0031】本明細書で開示するように、本発明によるセキュリティ問題に対応するシステムは、2つの別々の不揮発性消去可能メモリ素子、すなわちEEPROMとCOMS RAMを有する。これは一つには、本発明の時点でEEPROMが消去と書込みのサイクル数に関して寿命が限られているのに対して、PAPの状態およびPAPの正しい入力と、少なくとも万一のシステム・エンクロージャの無許可の開放状態を示す標識を何度も消去し書き込まなければならない可能性があるためである。したがって、本明細書で述べる機構は、現在使用可能な技術に対応するために、第1と第2の消去可能メモリ素子に分けられている。しかし、技術が許す場合、またはシステム設計者が以下で述べる制約を容認することを厭わない場合には、この2通りの形態の関連データを単一の消去可能メモリ素子に記憶することも可能であると企図される。

【0032】図4に、従来の電源制御装置すなわち「オン／オフ」スイッチ61と、従来の電源62と、主カバー15やケーブル接続カバー16などのエンクロージャ・カバーの開放または取り外しに応答して導通状態を変えるスイッチと、キーロック・スイッチ64との間の特定の関係を図示する。本発明の図示してある態様では、エンクロージャ・カバーの開放時または取り外し時に状態を変えるスイッチの数は2個である。すなわち、主カバー15の取り外しに応答するスイッチ65（図4、図5、および図6）と、ケーブル接続カバー16の取り外しに応答するスイッチ66（図4、図5、および図7）である。各スイッチは2つの構成要素を有し、一方は常時開（それぞれ65aおよび66a）であり、他方は常時閉（それぞれ65bおよび66b）である。第2のスイッチ66はケーブル接続カバー16がそうであるように、任意選択である。しかし、本明細書の開示を慎重に考慮すれば明らかになる通り、この任意選択のカバーとスイッチがあることによって、システムの一層徹底的なセキュリティ制御が保証される。

【0033】カバー・スイッチ65および66の常時開接点の組は、主電源スイッチ61および電源62（図4）に直列接続されている。したがって、カバーが取り外された状態でシステム10に「電源投入」を行おうとすると、接点の組65aおよび66aが開いてシステムが動作しないようにする。カバーが所定の位置にあると、接点の組は閉じたままになり、通常のシステム動作を開始することができる。

【0034】カバー・スイッチ65および66の常時閉接点の組は、キーロック・スイッチ64とRTCおよびCMOSメモリ68とに直列接続されている。常時閉接点の組65bおよび66bは、カバー15、16の存在によって開いたままに維持され、これらのカバーが取り外されると閉じる。キーロック・スイッチ64は、コンピュータ・システム10に通常設けられているエンクロージャ・ロックのロック時に常時閉状態に維持される。RTCおよびCMOSメモリの一部を付勢することになる電流に対してこの3組の接点によって接地への代替経路が提供され、システムがエンクロージャ・ロック状態にあるときにカバーの無許可の取り外しがあると、そのメモリのセグメントを弁別的な状態（すべて「1」など）に設定する効果を生ずる。メモリ内のそのセグメントがPOSTによって検査されるため、そのセグメントが弁別的な状態に設定されると、構成エラー信号が生成され、システム・セキュリティ侵害の試み（成功と不成功とを問わず）が行われたことを知らせる警報がシステム所有者に出される。

【0035】キーロック・スイッチ64および主エンクロージャ・カバー・スイッチ65は、主エンクロージャ・カバー15内に設けられているロックに対して適切な位置関係になるようにして、前面カード・ガイド部材69（図2および図6）上に取り付けることが好ましい。前面カード・ガイド部材は、コンピュータ・システム・フレーム内の、カバー・スイッチ65の作動レバー70が、直立前面フレーム部材の開口部を通って突き出し、カバー15が存在するときにカバー15によって作動してシステム・エンクロージャを閉じるように配置される位置に取り付ける。

【0036】ケーブル・カバー・スイッチ66は、ケーブル・カバー16に取り付けられたラッチ部材によって作動する位置に、エンクロージャ・カバー15上に設けられているものと同様の手動操作可能なキーロックの制御によって回転することができるようにして、システム・フレームの背面パネル上に取り付けることが好ましい。任意選択のケーブル・カバー16を使用する場合（システムの完全なセキュリティを所望するか必要とする場合）、カバーを背面パネルにラッチまたはロックすると、ラッチ部材がそれに関連する常時開接点の組66aを閉じ、常時閉接点の組66bを開く。

【0037】前述および後述のセキュリティ機構と保全

機構は、以前に提案したパーソナル・コンピュータ・セキュリティ機構である電源投入パスワード（POP）とは独立して機能する。これらの追加のセキュリティおよび保全機構は、オレンジ・ブックなどの適用規制に基づくオペレーティング・システム認証のための安全保護されたプラットフォームを提供する。システムを安全保護モードにするための追加のパスワードが必要である。このパスワードを本明細書では「特権アクセス・パスワード（PAP）」と呼ぶ。他のパーソナル・コンピュータ・システムとの互換性を維持するために、POPも継続してサポートされる。本明細書の説明では、EEPROM、オプション・スイッチ、および不正アクセス明示カバーを有するパーソナル・コンピュータ・システム上で実行されるPOSTおよびパスワード・ユーティリティに関係する範囲でセキュリティ機構と保全機構を扱う。

【0038】パスワード・セキュリティは、システム・ハードウェア機構、EEPROM、セキュリティ・スイッチ、および不正アクセス明示カバー・スイッチ、ファームウェア、POST、およびシステム・ソフトウェア・パスワード・ユーティリティによって実施される。PAPがインストールされると、システムは安全保護モードになる。PAPはEEPROMに保存される。PAPのバックアップ・コピーもEEPROMで維持される。これは、PAPのインストール、変更あるいは除去中に電源障害が起こった場合にPAPが偶発的に失われるのを防ぐために行われる。POPおよび、少なくとも、PAP（インストールされている場合）の妥当性を示す特定のビットがCMOS RTCに記憶される。CMOS RTCとEEPROMで保持されているデータの変更は、互いに独立している。

【0039】EEPROM内のビットは、更新シーケンスで電源異常が起こった正確な位置をPOSTに知らせ、可能な場合にはシステム・ボード交換状況から回復させる状態機械として使用される。パスワード・ユーティリティは、更新標識フィールド、すなわち、PAPへのアクセス中に使用される2ビット状態機械を維持する。パスワード変更中に電源異常が発生した場合、電源が回復されると、POSTがこの状態機械を検査する（POSTは実際には電源投入時に常にこの状態機械を検査する）。PAPの更新に成功している場合（「00」状態）、POSTは通常の方式で処理を進める。電源が失われる前に更新が開始されている場合（「01」状態）、POSTは有効なバックアップPAPの有無を調べる。有効な場合、POSTはそのバックアップPAPを1次PAPの記憶域にコピーする。1次PAPの更新に成功している場合（「10」状態）、POSTはその1次PAP（新しいPAP）を使用して、システム・リファレンス・ディスケットを使用する試行またはシステム区画をブートする試行の妥当性検査を行う。POSTはバックアップPAPが無効であるものとみなす。この場合、POSTは1次PAPをバックアップPAPにコピーする。オプション・スイッチまたはセキュリティ・スイッチがロック解除位置または書込み可能位置になっていない場合、エラーが表示される。システム所有者は、カバーをロック解除して、セキュリティ・スイッチの位置を変更することによって介入する必要がある。

【0040】バックアップPAPの更新に成功している場合（「11」状態）、1次PAPとバックアップPAPの両方が有効であるとみなされ、POSTはユーザによるPAPの入力を確認する前に、1次PAPの妥当性を検査する。

【0041】前述のように、POPはCMOSメモリで維持される。PAPのパスワード標識として使用するためにCMOSメモリで2ビットが維持される。一方の標識は、システムが安全保護モードになっている（PAPがインストールされている）ことを示すために使用される。もう一方の標識は、初期電源投入時、すなわちコールド・ブート時にPAPが入力されたことを示す。この2つの標識は、コールド・ブート時にのみ初期設定され、セットされる。インストールされているPAPの入力の成功を必要とするシステム・リファレンス・ディスケットまたはシステム区画のブートを行わない限り、これらの標識はIPLの前に書込み保護される。POPの変更と標識の変更は、EEPROに記憶されているPAPの変更とは独立している。しかし、CMOSメモリ内での変更は、セキュリティ侵害を示している可能性があり、回復のために有効なPAPを入力してオペレーティング・システムのロードを可能にする必要がある。

【0042】パスワードへの無許可のアクセスを防止するために、オペレーティング・システムをブートする初期プログラム・ロード（IPL）の前にIPLデバイス・ブート・リスト、EEPROM CRC、およびすべての標識がロックされる。これらの領域をロック・アウトするために、POSTは、システムの電源をオフにしない限りリセットすることができない特別なハードウェア・ラッチを設定する。POSTのステージIの最初（初期電源投入時）に、POSTはEEPROMがロックされているか否かを調べる。ロックされている場合、ハードウェアが機能不能であるため、POSTはエラーを表示し、システムを停止させる。システム・ボードの交換を必要とする可能性があるこの状況を修復するために、システム所有者が介入する必要がある。1つの態様では、システムが不正アクセスされた場合、RTCおよび制御レジスタに関連するCMOS内のRAM記憶域の最初の14バイトは影響を受けない。上記で簡単に述べたように、CMOSのうちのそのセグメントはすべて「1」（2進値の1）に設定される。この条件が検出されると、POSTは適切なエラーを表示する。他の態様では、1ビットだけを不正アクセスを示す状態に設定することができる。いずれの場合も、状況を修復するためにシステム所有者／許可ユーザが介入する必要があり、それにはシステム・リファレンス・ディスケットまたはシステム区画からブートするよう求めるパスワード・プロンプトに対してPAPを入力するか、システム・ボードを再構成することを必要とする可能性がある。

【0043】システム所有者がPAPを忘れた場合、影響を受けるシステム・ボードを交換する必要がある。

【0044】POPを忘れた場合は、システム所有者はカバーを空けて、システム・ボード上のもう1つのスイッチを切り換えてCMOS内のPOPの内容を破壊してから、PAP（インストールされている場合）を入力してシステム・リファレンス・ディスケットまたはシステム区画をブートしてパスワード・ユーティリティを実行し、POPを再インストールすることができる。

【0045】いずれのパスワードもインストールされていない状態でシステムに電源を入れると、POSTはパスワードを求めるプロンプトを出さない。しかし、システム・リファレンス・ディスケットが存在しないか、またはシステム区画ブートを要求しないかまたは存在しない場合、POSTはPAP、バックアップPAP、IPLデバイス・ブート・リスト、EEPROM CRC、およびすべての標識をロックする。これは、これらの領域への偶発的または悪意あるアクセスを防止するために行われる。システム・リファレンス・ディスケットが存在するか、システム区画ブートを要求された場合、これらの場所はロック解除されたままで、システム所有者が安全保護モードを呼び出すことができるようにする。POPはインストールされているがPAPがインストールされていない状態でシステムに電源を入れた場合、POSTは状態機械を検査してから、POPパスワード・チェックサムを検証する。チェックサムが正しくない場合、POSTはCMOS内のPOPを消去し、パスワードを求めるプロンプトを出さない。正しい場合は、POSTはパスワードを求めるプロンプトを出す。システム・リファレンス・ディスケットが存在しないか、システム区画ブートが要求されない場合、PAP、バックアップPAP、IPLデバイス・ブート・リスト、EEPROM CRC、およびすべての標識がロックされ、アクセスすることができないようにする。

【0046】有効なPAPがインストールされているが（安全保護モード）POPがインストールされていない状態でシステムに電源を入れた場合、POSTはPAPチェックサムを検証する。チェックサムが正しければ、POSTはシステム・リファレンス・ディスケットが存在するかシステム区画ブートが要求された場合にユーザに対してPAPを入力するよう求めるプロンプトを出す。正しくない場合は、POSTはパスワードの入力を求めず、POP、PAP、バックアップPAP、IPLデバイス・ブート・リスト、EEPROM CRC、およびすべての標識がロックされて、アクセスすることができなくなる。PAPチェックサムが正しくない場合、エラーが表示され、システムは停止する。これは、EEPROMが障害を起こしたときに前に安全保護モードになっていたシステムへの無保護アクセスを、POSTが偶発的にユーザに与える可能性のある状態を防止するためである。システム・ボードを交換しなければならない可能性のあるこの状況を修復するために、システム所有者の介入が必要になる。

【0047】有効なPAPと有効なPOPがインストールされている状態でシステムに電源を入れると、POSTはユーザにパスワードの入力を求めるプロンプトを出す。POPを入力した場合、POSTはシステム・リファレンス・ディスケットまたはシステム区画からはブートしない。システムは、既存のIPLデバイス・リストを使用しなければブートすることができない。プロンプトに対してPOPではなくPAPを入力した場合、ユーザはシステム・リファレンス・ディスケット、システム区画、IBLディスケット、または通常のIPLデバイス・リストからブートすることができる。初期電源投入時にPAPの入力に成功したことを示す標識が設定され、その電源投入セッションの後の方でシステム・リファレンス・ディスケットまたはシステム区画ブートを行うことができるようになる。POSTはソフト・リブートの後ではユーザにパスワードの入力を求めず、したがってPAPの入力成功標識とその保護は不要である。

【0048】簡単に言うと、コールド・スタート時にユーザがシステム・リファレンス・ディスケットまたはシステム区画からブートすることができる場合、POP、PAP、バックアップPAP、IPLデバイス・ブート・リスト、EEPROM CRC、およびすべての標識はロック解除されたままになる。この条件によって、トラステッド・ソフトウェア（すなわちシステム・リファレンス・ディスケット）と許可ユーザはシステムのセキュリティ・パラメータにアクセスすることができるようになる。POSTはいずれかのパスワードが正しく入力されていることを検証した後、確認アイコンを表示してその入力に肯定応答を行う。ネットワーク・サーバ（不在スタート）モードが活動状態のときには、POSTは前述のようにPOPを求めるプロンプトをスキップする。

【0049】上記のシナリオのフローチャート論理は、図8ないし図15に記載されており、図を簡単にするために、特定のステップ間のリンクは1文字表示が入ったプロセス・ブロックで示してある。

【0050】ネットワーク・サーバ（不在開始）モードがインストールされているシステムは、ターゲット・オペレーティング・システムのブートまでのブート・プロセスを完全に行うが、POPを使用してキーボードはロックされる。しかし、システム・リファレンス・ディスケットが存在するかシステム区画ブートを要求した場合

は、パスワード・プロンプトが表示されて、所有者はＰＡＰを入力することができ、システムの制御を再び獲得することができる。システムが安全保護状態になっており、キーボードがすでにロック・アウトされた後でユーザがシステム・リファレンス・ディスケットまたはシステム区画からのブートを行いたい場合は、ユーザはシステムの電源を遮断し、システム・リファレンス・ディスケットをディスケット・ドライブに入れて電源オフ状態からコールド・ブートを開始しなければならない。

【００５１】ＰＯＳＴ変更に関係して、パスワード・ユーティリティはＰＡＰのサポートを含んでいなければならない。ユーティリティはＰＡＰのインストール、変更、および除去をサポートし、この３つの機能をオプション・スイッチまたはセキュリティ・スイッチの位置と連動させる。セキュリティ・スイッチは許可ユーザがＰＡＰを設定しようとするまでロック位置のままになっていなければならない。ＰＡＰを設定する時点で、ユーザはシステム・カバーを取り外し、セキュリティ・スイッチをロック解除（変更）位置に移動しなければならず、それからＰＡＰを設定することができる。セキュリティ・スイッチがロック解除位置にあるとき、ＥＥＰＲＯＭの外部のハードウェア論理回路がＰＡＰをＥＥＰＲＯＭに記憶することができるようにする。セキュリティ・スイッチがロック位置にあるとき、外部ハードウェア論理回路はＥＥＰＲＯＭ内のＰＡＰ記憶場所にいかなる変更も加えることができないようにする。セキュリティ・スイッチがロック位置にあるときに許可ユーザがＰＡＰを変更しようとした場合、適切なメッセージが表示される。また、ＰＡＰを除去した後でセキュリティ・スイッチをロック位置に戻すようにユーザに注意するメッセージも表示される。パスワード・ユーティリティには許可ユーザがＰＯＰと同じＰＡＰを設定するのを禁止する付加的な安全機構も組み込まれている。ＰＡＰの設定または変更を行うと、検査が行われ、新しいＰＡＰがシステムの現行ＰＯＰと等しくならないようにする。また、ＰＡＰを変更または除去するときは、現行ＰＡＰを知っていなければならない。

【００５２】パーソナル・コンピュータ・システムは最初に、セキュリティ・スイッチがロック位置にあり、不正アクセス明示カバーがロックされた状態で出荷されることが企図される。これは、システム所有者以外の人がシステムを安全保護モードに設定するのを防止するためである。ＰＯＰとは異なり、ＰＡＰはハードウェア操作によって消去することができない。ＰＡＰを忘れたり無許可ユーザがシステムを安全保護モードに設定した場合は、システム・ボードを交換しなければならない。

【００５３】本明細書で述べるメモリ素子、スイッチ、およびその相互接続は、この説明では「セキュリティ機構要素」と呼び、列挙した構成要素がコンピュータ・システムのうちで、本明細書で説明するセキュリティ機構を具体的にイネーブルする要素であることを示している。

【００５４】おわかりのように、本明細書で説明するセキュリティ機構を有するパーソナル・コンピュータ・システムは、本明細書で説明するセキュリティ対策を破ろうとする無許可ユーザによる攻撃の対象となる。１つの予想される攻撃形態は、カバー１５とシャーシ１９によって作られているエンクロージャ内に画定されている開口部からの単純な物理的攻撃であろう。このような開口部は、たとえば、エンクロージャを通る冷却空気の流れのため、フロッピィ・ディスクおよびその他のディジタル信号記憶媒体の挿入と取り外しのため、ケーブルなどの装着のため、および所定の位置にボルトまたはねじで固定される装備品や付属部品の（製造時または製造後の）装着のために設けられている。このような開口部のいずれも、前述のセキュリティ機構を回避しようとする無許可ユーザがプローブを差し込む機会を与える可能性がある。したがって、知識のある攻撃者はＰＡＰまたはＰＯＰのデータが記憶されているメモリ素子からＰＡＰまたはＰＯＰを消去しようとしたり、前述のインターロック・スイッチ配置構成を破壊するような方法で電力を供給しようとしたりする可能性がある。

【００５５】このような攻撃からの保護の解決策は、コンピュータ・システムのエンクロージャ内に配置するメモリ素子とスイッチを、開口部からプローブを差し込んでメモリ素子またはスイッチの１つの動作に影響を与えようとするパーソナル・コンピュータ・システムの無許可ユーザが届かない位置に取り付けることである。プローブを差し込まれる開口部は、冷却空気を通す通風孔であるか、攻撃者側が巧妙な場合には、前述のその他の様々な開口部の１つである可能性がある。プローブは、曲げたペーパー・クリップなどの単純な道具や、前述のセキュリティ機構要素に届くように、またはセキュリティ機構要素の正常な動作を無効にして無許可ユーザが普通なら保護されているはずのデータへのアクセスを獲得することができるようにする何らかの形のエネルギー（電気、音、放射線）を放射するように特別に作られたより精巧な仕掛けである場合がある。

【００５６】前述のようなセキュリティ機構要素は、機械プローブ攻撃ができないようにエンクロージャ開口部から離れた場所に配置するか、または非機密的性質の他のコンピュータ要素によって遮蔽された位置に配置することによって、前述のタイプのプローブ攻撃から保護することができる。セキュリティ機構要素を接続し、場合によってはセキュリティ機能に関係するディジタル信号を伝送する信号経路は、多層プリント回路基盤の内部に配置することによって攻撃から保護することができる。コンピュータ・エンクロージャに画定されている開口部は、曲がりくねった通路として構成するか、非機密要素によって遮蔽することによって、攻撃アクセスを制限または防止するように構成することができる。

【００５７】本発明は、移動を検出する任意選択機能をさらに備えた、前述のタイプの従来技術のコンピュータ・システムを企図している。移動監視スイッチによってコンピュータ・システムの無許可の移動が検出されると、前述の従来技術の不正アクセス明示機構、または好ましくは類似しているが別個の移動監視機構を起動して、システムを機能不能状態にすることができる。移動とは、固定されたシステムをその平常の位置合わせされた位置、すなわちデスクトップまたはラップトップの場合は水平、床置きシステムの場合は垂直の位置から物理的に移動することであると定義される。無許可の移動とは、この新規のセキュリティ機構がイネーブルされる場合の移動と定義される。本発明を詳細に説明するために、図２、図４、および図１６ないし１９のハードウェアと、図８ないし１５のフローチャートに注目されたい。

【００５８】図１６および図１７には、デスクトップ・システムと床置きシステムの平常位置合わせされている、それぞれの水平位置と垂直位置が図示されている。図１８には、コンピュータ１０内の水平面のＸ軸およびＺ軸の適切な固定位置に取り付けられた移動検出スイッチ１００～１０３の１つの好ましい実施例が図示されている。

【００５９】図１９には、机上に水平位置に、または床に垂直位置に設置することができるコンピュータ１０の、スイッチ１００～１０３が適切に取り付けられた駆動要素１０５が図示されている。この要素１０５は、図２では固定位置に取り付けられている様子が示されており、デスクトップ位置または床置き位置にあるコンピュータ１０用にスイッチ１００～１０３が水平に配置された２つの位置の間で９０度回転する。

【００６０】スイッチ１００～１０３は、常時開位置に維持されていて、各スイッチの電気リード端に水銀が流れると閉じる水銀リード・スイッチであることが好ましい。Ｚ軸上の１対のスイッチ１００および１０１とＸ軸上の１対のスイッチ１０２および１０３は、それぞれの電気出力リードが向かい合った方向にあり、Ｘ軸またはＺ軸方向に傾くと少なくとも１つのスイッチが閉じるように取り付けられている。これらのスイッチおよびそれらとリアル・タイム・クロックＲＴＣおよびＣＭＯＳ ＲＡＭ６８との接続を図４に示す。

【００６１】具体的には、電界効果トランジスタ（ＭＯＳＦＥＴ）１０６の付勢または減勢状態に応じて、スイッチ１００、１０１、１０２、および１０３の接点の組１００ａ、１０１ａ、１０２ａ、および１０３ａ（図４）によって、バッテリ電圧または地電位がＲＴＣおよびＣＭＯＳ ＲＡＭ６８に接続される。トランジスタ１０６がオフのとき、接点１００ａ～１０３ａにバッテリ電圧が加えられ、トランジスタがオンになると、接点１００ａ～１０３ａに地電位が加えられる。後述のように移動検出セキュリティ機構がイネーブルされると、トランジスタ１０６の入力端１０７に適切な信号が送られて、トランジスタ１０６をオンにする。

【００６２】垂直方向（図１８のＹ軸）の移動の移動検出手段がないことに注目されたい。好ましい実施例では、垂直移動検出は余分であると考えられるため、すなわち万一盗難があった場合にはＸ軸またはＺ軸の傾斜が避けられないと考えられるため、垂直移動検出は省かれる。しかし、当業者なら、たとえばデスクトップ・コンピュータ１０の基部から突出してデスクトップとかみ合い、接点（図示せず）を常時開状態に維持するように調整されたばね負荷ピン（図示せず）によって、垂直移動の検出機能も備えることができることは明らかである。コンピュータ１０を持ち上げると、ピンがコンピュータ１０の基部から突出し、ピンに関連する接点が閉じてＲＴＣおよびＣＭＯＳ ＲＡＭ６８に接地が結合される。

【００６３】コンピュータ１０は、ケーブル・アンド・ロック（図示せず）などの固定機構を使用して据え付け、コンピュータ・システムの物理的な取り外しを抑止することが好ましい。固定機構は、移動検出機構（移動監視機構と呼ぶ場合もある）をイネーブルする前に取り付けなければならない。そうしないと、固定機構の取り付け中の移動のために、移動検出機構が作動する可能性がある。

【００６４】本発明のより簡略化された態様（ただし本発明の好ましい実施例ではない）では、線１０７（図４）に信号を送ってトランジスタ１０６をオンにし、それによって接点の組１００ａ～１０３ａに地電位を加える機能を含む様々な機能を実行するユーティリティを呼び出すことによって移動監視機構をイネーブルする。その後で接点の組１００ａ～１０３ａのうちの１つがコンピュータ・システム１０の無許可の移動のために閉じた場合、システムからカバーが取り外されたときに不正アクセス明示スイッチ６５ｂ、６６ｂによって「１」に設定されるＲＴＣおよびＣＭＯＳメモリ６８の同じセグメントに地電位が加えられる。したがって、移動監視機構がイネーブルされているときのシステムの無許可の移動と、不正アクセス明示機構がイネーブルされているときのカバーの無許可の取り外しは両方とも、同じ構成エラーを引き起こし、その後システムはそれを、関連出願番号第０７／８８９３２５号の従来技術のセキュリティ機構に関連して前述した電源オフ、電源オン手順時に、同じ方式で処理する。

【００６５】しかし、本発明の好ましい実施例では、システムの無許可の移動によって引き起こされた構成エラーと不正アクセス明示スイッチの作動によって引き起こされた構成エラーとを区別して、適切な監査証跡を維持することが望ましい。この好ましい実施例は、無許可の移動の検出後、電源を切った後で電源投入時にＰＯＰの

入力に成功することによって移動機構をイネーブルしてコンピュータ・システムの動作を再確立することができることを企図している。さらに、移動監視機構がイネーブルされている間のシステムの移動によってコンピュータ・システムの正常動作が中断されない。POPの入力に成功してシステムの動作を再確立する必要があるのは、その後で電源を切ってから電源を投入するときだけである。これらの機能が好ましいのは、通常ユーザによるコンピュータ・システムの不注意の移動が容易に起こる可能性があり、その結果システムの通常の使用が無用に中断されると非生産的になるからである。

【００６６】したがって、好ましい実施例は、記憶装置６８の所定のセグメントの１ビットが機構がイネーブルされている状態でのカバーの不正アクセス・スイッチ６５、６６の作動を示し、第２の移動検出ビット（またはフラグ）が機構がイネーブルされている状態での移動検出スイッチ１００～１０３の作動を示すように指定されることを企図する。スイッチ６５、６６および１００～１０３は、図４に示すように作動するとこれらのビット（またはフラグ）を「１」に設定する。

【００６７】コンピュータ・システムの移動後、電源を切った後の電源投入時に、POSTはスイッチ１００～１０３によって移動検出フラグが「１」に設定されたか否かを判断し、POPの入力が成功するとシステム動作を再確立する。すなわち、DASDからオペレーティング・システムをブートすることができるようにする。

【００６８】したがって、POSTは不正アクセス明示機構（記憶装置６８の所定のセグメントの所定のビット位置に設定されている「１」）が作動しているか否かを調べて判断し、記憶装置６８内の別の所定のビット位置も「１」に設定されているか否かを調べることによって無許可の移動が検出されたか否かを判断する。

【００６９】好ましい実施例の不正アクセス明示スイッチ６５、６６は、記憶装置６８の所定のセグメント内の最初に述べた第１のビットを設定し、移動監視スイッチ１００～１０３は所定のセグメント内の第２のビットを設定する。

【００７０】好ましい実施例では、移動監視機構には２つの動作モードがある。各モードをイネーブルするには、PAPがインストールされている必要がある。一方のモードは、PAPのみがインストールされている場合にイネーブルされ、他方のモードはPAPとPOPの両方がインストールされている場合にイネーブルされる。

【００７１】移動監視機能をイネーブルする前に、少なくともPAPをインストールしてシステムを安全保護モードにしなければならない。さらに、コンピュータは不正アクセス明示カバー、固定機能、（従来の技術で定義されている）システム・アクセス開口部を通した安全機構の破壊を防止する手段、および不揮発性記憶装置６８内の　込み保護領域を備えることが好ましい。これらの機構がないと、システム所有者または許可ユーザによる使用事象の監査証跡が損なわれることになる。

【００７２】移動監視機構をイネーブルするために、ユーザはユーティリティを呼び出す。このユーティリティはシステムに付属して提供され、ユーザが移動監視機構をイネーブルまたはディスエーブルすることができるようにする。このユーティリティはオペレーティング・システムのコマンド・プロンプトから実行される。ユーザがこの機構をイネーブルすることを選択した場合、CMOSおよびRTC記憶装置６８内の書込み保護フィールドが、移動監視を実行することを示すように設定され、トランジスタ１０６（図４）がオンになる。移動監視をイネーブルした場合、ユーザは移動検出をディスエーブルするまでシステムを置いておく物理的位置にシステムを置いた状態で電源を切らなければならない。電源がオンのままでこの機構がイネーブルされていると、オペレーティング・システムはシステム資源およびデータへの無許可のアクセスが行われないように保護しなければならない。オペレーティング・システムには、移動監視機構からの割込みによって無許可の移動が通知される。

【００７３】この機構をディスエーブルした場合（図４のトランジスタ１０６がオフの場合）、ユーザはシステムを自由に移動させることができる。固定機構は移動検出機構をイネーブルする前に取り付けなければならない。そうでないと、たとえばケーブル・アンド・ロックなどの固定機構を取り付けている間の移動によって、移動検出機構が不正アクセス明示機構を作動させる可能性がある。機構をイネーブルするユーティリティが呼び出されると、線１０７上の信号によってトランジスタ１０６が付勢され、接点１００ａ～１０３ａに地電位が加えられる。

【００７４】以下に、PAPとPOPがインストールされているモードについて説明する。

【００７５】電源オフ状態からの次の電源投入時に、POSTは不正アクセス明示機構をイネーブルするために不揮発性記憶装置が活動状態になっているか、移動監視機構または不正アクセス明示既往（あるいはその他のセキュリティ機構）が侵害されていないか、移動が検出されていないか、移動検出機構がイネーブルされているか、およびカバーの不正アクセス機構が侵害されていないかを、不揮発性記憶装置に設定されているコンピュータ・システム状況を示す様々なビットまたはフラグを使用して判断する。

【００７６】移動が検出され、移動監視機構がイネーブルされていることが判明した場合、POSTはCMOS記憶装置６８内の移動検出フラグを設定してPOPの入力を求めるプロンプトを出す。POPが正しく入力された場合、POSTはシステムが移動されたことを示すメッセージを表示する。POPが損なわれている場合、すなわちバッテリが切れているかまたはPOPが正しく入力されていない場合、POSTはそれ以上処理を進めない。誤ったPOPの入力が３回試行されると、POSTはCMOS６８内の標識を自ら設定して、次の電力投入時にPAPの入力を求めるプロンプトを出す。POSTはシステムをディスエーブルする。システムを再起動するためには、システムの電源を切ってから電源を入れて、PAPの入力を求めるプロンプトを表示させる必要がある。PAPが正しく入力されるまでは、システムはブートせず、したがってシステムは非活動状態になる。POSTは、１つの電源投入セッションでPAPを正しく入力する試行が３回失敗するたびにシステムを非活動状態にする。PAPをもう一度入力できるようにするには、電源切断と電源投入の１サイクルが必要である。この状態が存在すると、そのユーザは、PAPを知らない場合、システムをシステム所有者または許可ユーザに返して再起動しなければならないことがある。移動検出機構をイネーブルし活動化している場所からシステムを除去した場合、システムを除去した人はPAPを知らない限り除去したシステムを使用してどのデータにもアクセスすることができなくなる。

【００７７】POP付きPAP動作モードは、移動システムのために構想された動作モードである。移動検出機構がイネーブルされていて無許可の移動が行われた場合、PAPのみの動作モードでのシステムのセットアップでは、ユーザはシステム所有者または許可ユーザを捜してPAPを入手しない限りシステムを再活動化することができない。これを行うことは、当該ユーザとPAPを知っている人の２人が物理的に異なる場所や異なる時間帯にいる可能性を考えると困難な場合がある。また、この事象が当該ユーザによってシステム所有者または許可ユーザに報告され、監査証跡の保全性を保証し、システム所有者が設定したセキュリティ方針の維持に役立てることも予想される。

【００７８】以下に、PAPのみがインストールされているモードについて説明する。

【００７９】電源オフ状態からの次の電源投入時に、POSTは移動検出がイネーブルされているかどうか、移動監視機構が活動化されているかどうかを調べる。両方の条件が満たされている場合、POSTはPAPの入力を求めるプロンプトを出す。PAPの誤った入力が３回試行されると、POSTはシステムをディスエーブルする。システムを再起動するためには、システムの電源を切ってから電源を投入してPAPの入力を求めるプロンプトを表示させる必要がある。PAPが正しく入力されるまではシステムはブートせず、従ってシステムは非活動状態になる。POSTは、１つの電源投入セッションでPAPを正しく入力する試行が３回失敗するたびにシステムを非活動状態にする。PAPをもう一度入力できるようにするには、電源切断と電源投入の１サイクルが必要である。この状態が存在すると、そのユーザは、PAPを知らない場合、システムをシステム所有者または許可ユーザに返して再起動しなければならないことがある。監視検出機構をイネーブルし活動化している場所からシステムを除去した場合、システムを除去した人はPAPを知らない限り除去したシステムを使用してどのデータにもアクセスすることができなくなる。

【００８０】以上、本明細　では本発明について、最も実際的で好ましいと考えられる実施例で示し、説明した。しかし、本発明の範囲内でこの実施例から逸脱することが可能であり、当業者には明白な変更が思いつくものと認められる。

【００８１】まとめとして、本発明の構成に関して以下の事項を開示する。

【００８２】（１）データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、常時閉じられているエンクロージャと、前記エンクロージャ内に実装され、活動状態と非活動状態への選択的活動化を行い、活動状態のときに特権アクセス・パスワードを受け取って記憶する消去可能メモリ素子と、前記消去可能メモリ素子に作動可能に接続され、前記消去可能メモリ素子を活動状態および非活動状態に設定するためにパーソナル・コンピュータ・システムのユーザによって手動設定可能な、前記エンクロージャ内に実装された手動操作可能なオプション・スイッチと、移動検出スイッチと、移動検出スイッチを選択的にイネーブルおよびディスエーブルする手段と、前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する前記移動検出スイッチと、移動検出スイッチを含み、前記移動検出スイッチがイネーブルされているときに前記移動検出スイッチの任意の切換えに応答して、コンピュータ・システムの電力投入の成功を妨げる手段と、前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、パスワードの入力と非入力および移動検出スイッチのイネーブル状態とディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含むシステム。

（２）システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化することを特徴とする、上記（１）に記載のパーソナル・コンピュータ・システム。

（３）消去可能メモリ素子が電源投入パスワードを受け取って記憶し、前記システム・プロセッサが移動検出スイッチの切換え後の電源投入中に、システムのユーザが電源投入パスワードの入力に成功するとシステムを活動化してシステム内に記憶されている特定のレベルのデー

タにアクセスすることができるようにすることを特徴とする、上記（1）に記載のパーソナル・コンピュータ・システム。

（4）前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、上記（3）に記載のパーソナル・コンピュータ・システム。

（5）システム・プロセッサが、消去可能メモリ素子内のいずれかのパスワードの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、上記（4）に記載のパーソナル・コンピュータ・システム。

（6）システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対して移動検出スイッチの切換えの標識を提供することを特徴とする、上記（1）に記載のパーソナル・コンピュータ・システム。

（7）移動検出スイッチが、エンクロージャ内の水平面に取り付けられた2対の水銀リード・スイッチを含み、1対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該2対の水銀リードスイッチの傾斜によって少なくとも1つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、上記（1）に記載のパーソナル・コンピュータ・システム。

（8）データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、常時閉じられているエンクロージャと、前記エンクロージャ内に実装され、活動状態と非活動状態への選択的活動化を行い、活動状態のときに電源投入パスワードと特権アクセス・パスワードを受け取って記憶する消去可能メモリ素子と、前記消去可能メモリ素子に作動可能に接続され、前記消去可能メモリ素子を活動状態および非活動状態に設定するためにパーソナル・コンピュータ・システムのユーザによって手動設定可能な、前記エンクロージャ内に実装された手動操作可能なオプション・スイッチと、前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されて前記エンクロージャの開放を検出する不正アクセス検出スイッチと、前記エンクロージャ内に取り付けられ、前記消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する移動検出スイッチと、移動検出スイッチを選択的にイネーブルおよびディスエーブルするプログラム被制御手段と、不正アクセス検出スイッチまたは前記移動検出スイッチがイネーブルされているときに不正アクセス検出スイッチまたは前記移動検出スイッチの切換えに応答して、コンピュータ・システムの電源投入の成功を妨げる手段と、前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、前記メモリ素子の活動状態と非活動状態、パスワードの入力と非入力、および移動検出スイッチのイネーブルとディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含む、パーソナル・コンピュータ・システム。

（9）前記システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにすることを特徴とする、上記（8）に記載のパーソナル・コンピュータ・システム。

（10）前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、上記（9）に記載のパーソナル・コンピュータ・システム。

（11）システム・プロセッサが、システムのユーザによるパスワードの1つの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、上記（10）に記載のパーソナル・コンピュータ・システム。

（12）システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対して移動検出スイッチの切換えの標識を提供することを特徴とする、上記（8）に記載のパーソナル・コンピュータ・システム。

（13）移動検出スイッチが、エンクロージャ内の水平面に取り付けられた2対の水銀リード・スイッチを含み、1対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該2対の水銀リードスイッチの傾斜によって少なくとも1つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、上記（8）に記載のパーソナル・コンピュータ・システム。

（14）データを受け取って保持し、システム内に保持されているデータを無許可のアクセスから安全保護することができるパーソナル・コンピュータ・システムであって、常時閉じられているエンクロージャと、移動検出スイッチと、移動検出スイッチを選択的にイネーブルおよびディスエーブルするプログラム被制御手段と、前記エンクロージャ内に実装され、活動状態と非活動状態に選択的に活動化され、活動状態のときに特権アクセス・

パスワードを受け取って記憶する第1の消去可能メモリ素子と、前記エンクロージャ内に取り付けられ、前記第1の消去可能メモリ素子に作動可能に接続されて、前記第1の消去可能メモリ素子を活動状態および非活動状態に設定するオプション・スイッチと、前記エンクロージャ内に実装され、電源投入パスワードおよび、移動検出スイッチのイネーブル状態と、第1の消去可能メモリ素子の状態と、記憶されている任意の電源投入パスワードおよび特権アクセス・パスワードの正しいインストールとを示すデータを受け取って記憶する第2の消去可能メモリ素子と、前記エンクロージャ内に取り付けられ、前記第2の消去可能メモリ素子に作動可能に接続されて前記エンクロージャの無許可の開放を検出する不正アクセス検出スイッチと、前記エンクロージャ内に取り付けられ、前記第2の消去可能メモリ素子に作動可能に接続されてコンピュータ・システムの無許可の移動を検出する前記移動検出スイッチと、特権アクセス・パスワードがインストールされている状態で効力を生じ、不正アクセス検出スイッチの切り換えに応答し、移動検出スイッチがイネーブルになっているときに移動検出スイッチの切り換えに応答して、コンピュータ・システムの電源投入の成功を妨げる手段と、前記エンクロージャ内に実装され、前記消去可能メモリ素子に作動可能に接続されて、移動検出スイッチのイネーブル状態とディスエーブル状態、および第1および第2の消去可能メモリ素子内の記憶されている任意の有効な特権アクセス・パスワードおよび記憶されている任意の有効な電源投入パスワードの入力と非入力を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するシステム・プロセッサとを含む、パーソナル・コンピュータ・システム。

（15）前記システム・プロセッサが、移動検出スイッチの切換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにすることを特徴とする、上記（14）に記載のパーソナル・コンピュータ・システム。

（16）前記システム・プロセッサが、電源投入パスワードの入力の試行の失敗の後に、システムの許可ユーザによる特権アクセス・パスワードの入力が成功するとシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにすることを特徴とする、上記（15）に記載のパーソナル・コンピュータ・システム。

（17）システム・プロセッサが、システムのユーザによるパスワードの1つの入力の成功に付随する正常なプログラムの実行を継続することを特徴とする、上記（16）に記載のパーソナル・コンピュータ・システム。

（18）システム・プロセッサが、システム所有者のための監査証跡を維持するためにシステム・ユーザに対してイネーブルされている移動検出スイッチの切換えの標識を提供することを特徴とする、上記（15）に記載のパーソナル・コンピュータ・システム。

（19）移動検出スイッチが、エンクロージャ内の水平面に取り付けられた2対の水銀リード・スイッチを含み、1対のそれぞれの水銀リード・スイッチが共通軸上に配置され、各対の軸が他方の対の軸から９０度の角度に配置され、各対の電気出力リードが向かい合った方向に配置されて、該2対の水銀リードスイッチの傾斜によって少なくとも1つの水銀リード・スイッチの切換えが行われるようになっていることを特徴とする、上記（14）に記載のパーソナル・コンピュータ・システム。

（20）エンクロージャと、エンクロージャ内に実装されたシステム・プロセッサと、エンクロージャ内に実装された選択的活動化が可能な消去可能メモリ素子と、エンクロージャ内に装着されてパーソナル・コンピュータ・システムのユーザが手動で設定することができる、メモリ素子を活動状態および非活動状態に設定する手動操作可能オプション・スイッチと、エンクロージャ内に装着され、エンクロージャの開放を検出する不正アクセス検出スイッチと、エンクロージャ内に装着され、コンピュータ・システムの平常稼働位置からの移動を検出する移動検出スイッチと、移動検出スイッチをイネーブル状態にするユーザ呼出し可能ユーティリティ・プログラムとを有するパーソナル・コンピュータ・システムを操作する方法であって、オプション・スイッチを手動で設定し、メモリ素子を活動状態に選択的に設定するステップと、活動メモリ素子に特権アクセス・パスワードを記憶するステップと、移動検出スイッチをイネーブルするユーティリティ・プログラムを呼び出すステップと、パスワードの入力と非入力および移動検出スイッチのイネーブル状態とディスエーブル状態を区別することによって、システム内に記憶されている少なくとも特定のレベルのデータへのアクセスを制御するステップと、不正アクセス検出スイッチの任意の切り換えに応答し、イネーブルされている移動検出スイッチの切換えに応答して、システムの電源投入を妨げるステップとを含む方法。

（21）メモリ素子に電源投入パスワードを記憶するステップと、移動検出スイッチの切り換え後の電源投入中に、システムのユーザによる電源投入パスワードの入力の成功に応答してシステムを再活動化してシステム内に記憶されている特定のレベルのデータにアクセスすることができるようにするステップとをさらに含むことを特徴とする、上記（20）に記載の方法。

（22）電源投入パスワード入力の試行の失敗の後に、システムのユーザによる特権アクセス・パスワードの入力の成功に応答してシステムを再活動化してシステム内に記憶されているすべてのレベルのデータにアクセスすることができるようにするステップをさらに含む、上記

（２０）に記載の方法。

【図面の簡単な説明】

【図１】本発明を実施するパーソナル・コンピュータの透視図である。

【図２】シャーシ、カバー、プレーナ・ボードを含み、それらの要素間の特定の関係を図示し、さらに、本発明のセキュリティ機構に関係する構成要素を含む、図１のパーソナル・コンピュータの特定の要素の分解透視図である。

【図３】図１および図２のパーソナル・コンピュータの特定の構成要素の配線略図である。

【図４】従来の技術のセキュリティ機構および本発明のセキュリティ機構に関係する、図１および図２のパーソナル・コンピュータの特定の構成要素を表す略図である。

【図５】従来の技術のセキュリティ機構および本発明のセキュリティ機構に関係する、図１および図２のパーソナル・コンピュータの特定の構成要素を表す略図である。

【図６】図４および図５に図示されている特定の構成要素の拡大透視図である。

【図７】図１、図２、図４、および図５のパーソナル・コンピュータの特定の任意選択構成要素を示す、図６と同様の図である。

【図８】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図９】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１０】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１１】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１２】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１３】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１４】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１５】本発明のセキュリティ機構に含まれる機能を組み込むために修正された従来の技術の不正アクセス明示セキュリティ機構による、使用可能なセキュリティ・オプションに含まれる特定の機能を示した概略フローチャートである。

【図１６】コンピュータ・システムがデスクトップ・コンピュータまたは床置きコンピュータとして動作することができる水平位置を示す図である。

【図１７】コンピュータ・システムがデスクトップ・コンピュータまたは床置きコンピュータとして動作することができる垂直位置を示す図である。

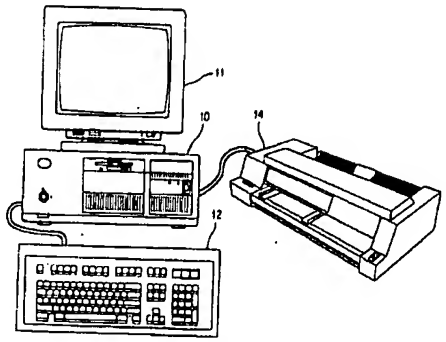
【図１８】移動監視スイッチを配置する水平Ｘ軸およびＺ軸を示す図である。

【図１９】垂直位置と水平位置のいずれかで使用することができるコンピュータで使用する回転可能支持構造体上の移動監視スイッチの取付けを示す図である。

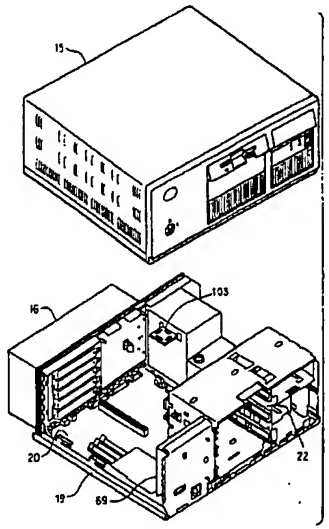
【符号の説明】

１５　主カバー
１６　ケーブル接続カバー
１９　シャーシ
２０　システム・プレーナ
２２　上部ベイ
４５　マイクロ・チャネル・アダプタ・カード
６１　オン／オフ・スイッチ
６２　電源
６４　キーロック・スイッチ
６５　カバー・スイッチ
６６　カバー・スイッチ
６８　ＣＭＯＳ　ＲＡＭ
６９　前面カード・ガイド部材
７０　作動レバー
１００　移動検出スイッチ
１０５　駆動要素
１０６　電界効果トランジスタ

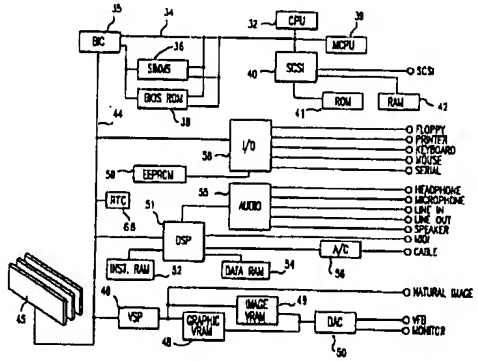
【図１】



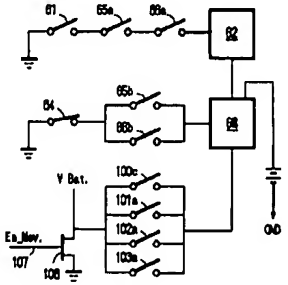
【図２】



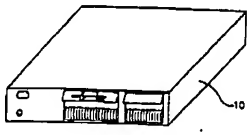
【図３】



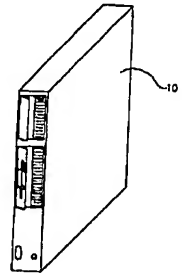
【図４】



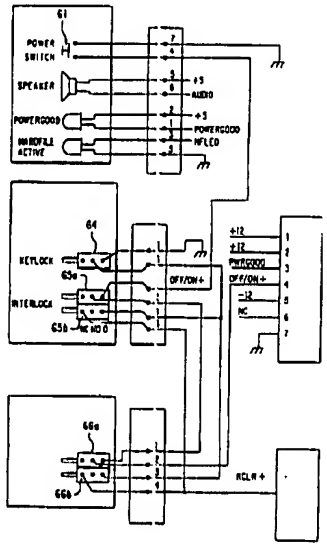
【図１６】



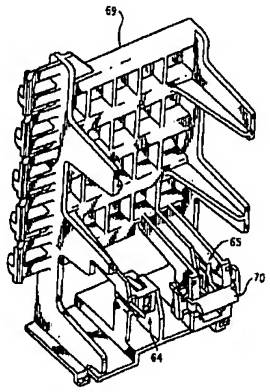
【図１７】



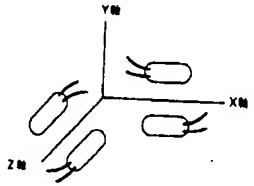
【図5】



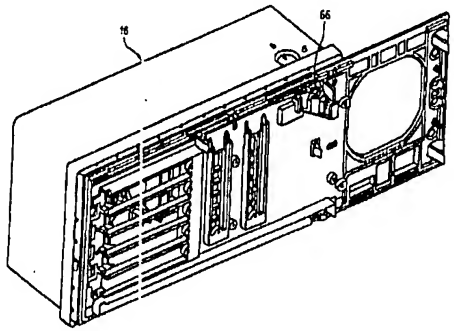
【図6】



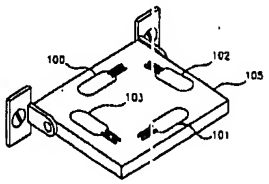
【図18】



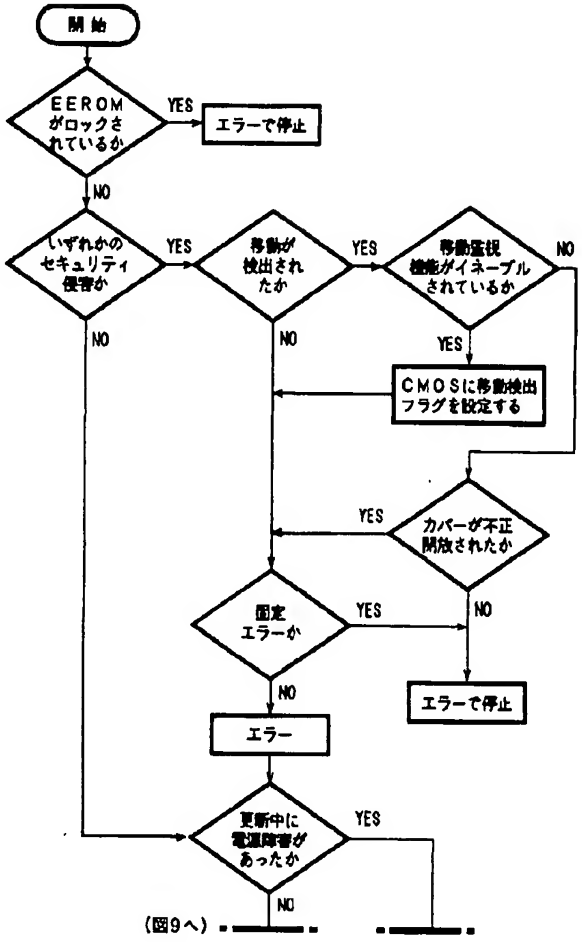
【図7】



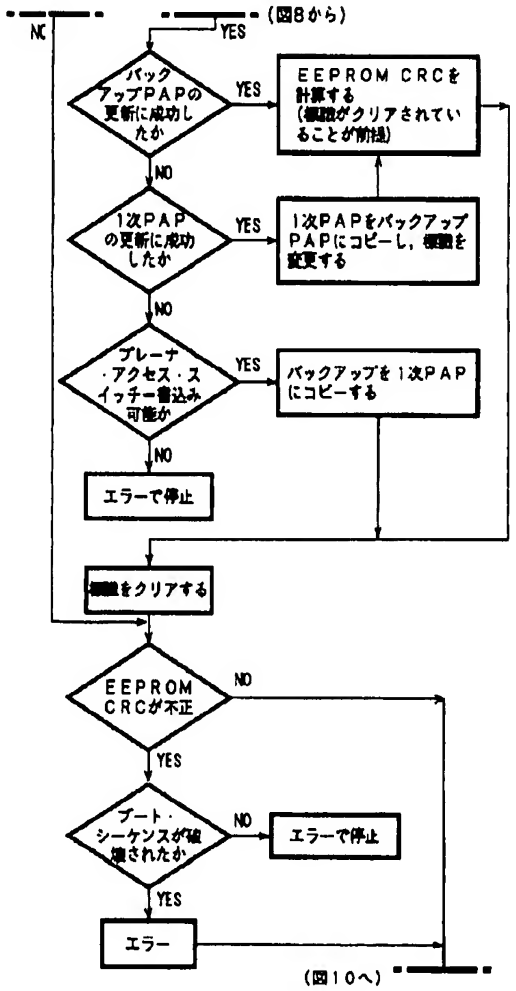
【図19】



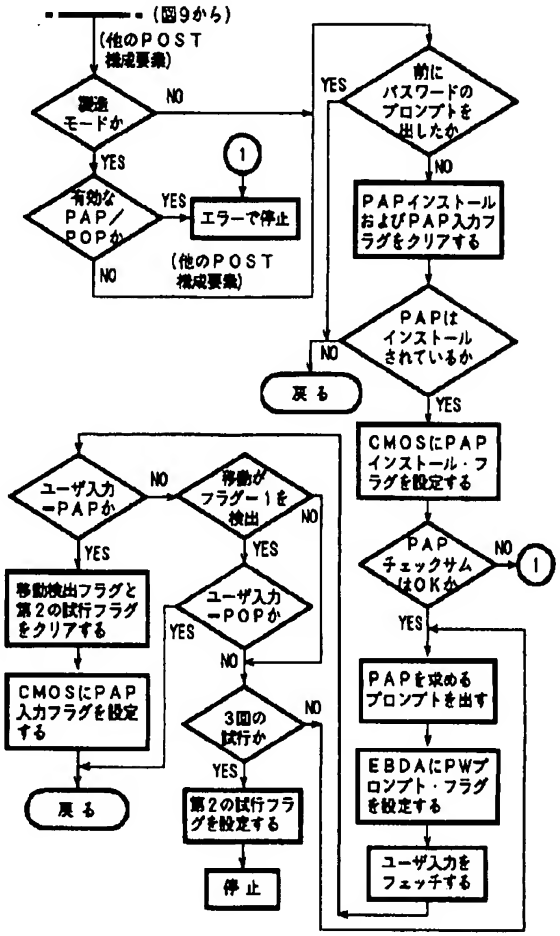
【図8】



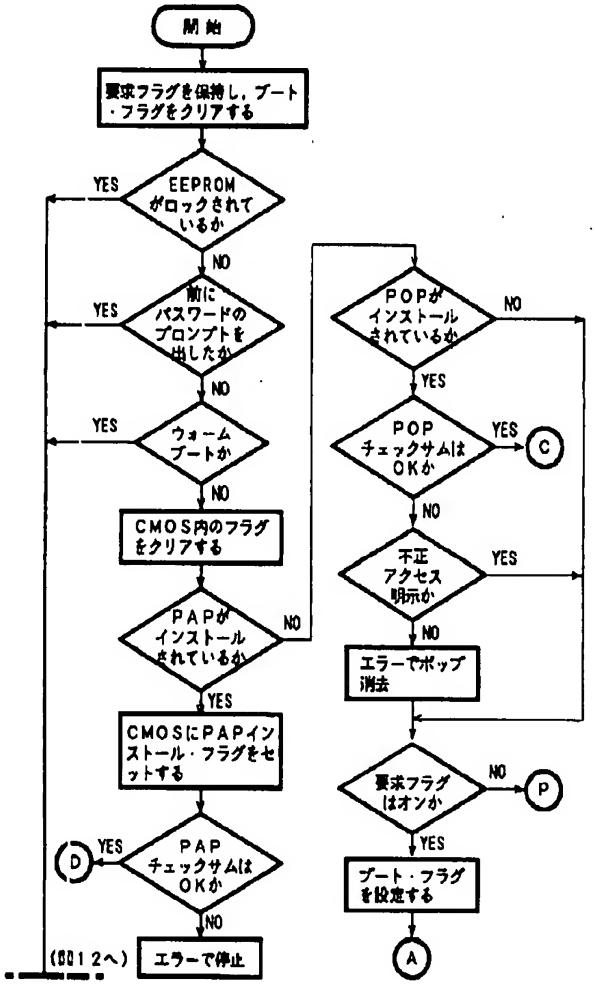
【図９】


(図8から)
NC
YES
バックアップPAPの更新に成功したか
YES
EEPROM CRCを計算する (標識がクリアされていることが前提)
NO
1次PAPの更新に成功したか
YES
1次PAPをバックアップPAPにコピーし，標識を変更する
NO
プレーナ・アクセス・スイッチー書込み可能か
YES
バックアップを1次PAPにコピーする
NO
エラーで停止
標識をクリアする
EEPROM CRCが不正
NO
YES
ブート・シーケンスが破壊されたか
NO
エラーで停止
YES
エラー
(図10へ)

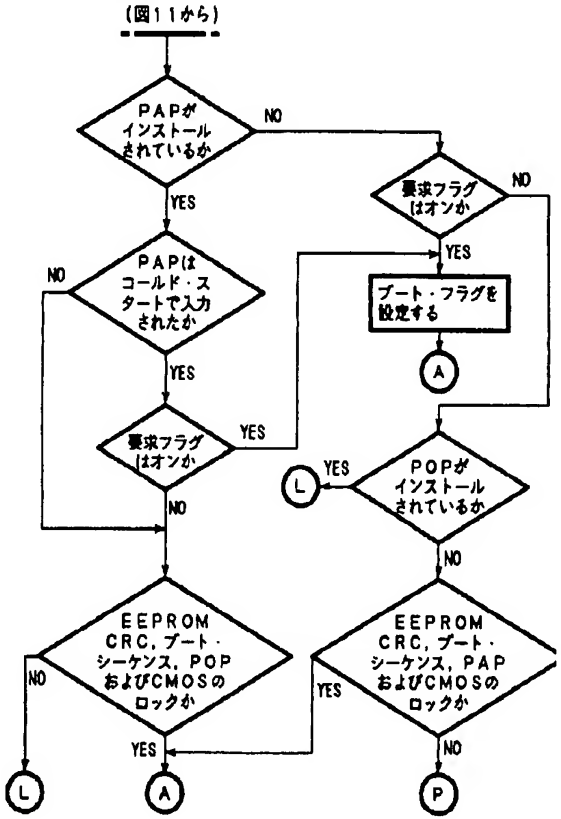
【図１０】


(図9から)
(他のPOST構成要素)
漫遊モードか
NO
YES
有効なPAP/POPか
YES
1
エラーで停止
NO
(他のPOST構成要素)
前にパスワードのプロンプトを出したか
YES
NO
PAPインストールおよびPAP入力フラグをクリアする
PAPはインストールされているか
NO
戻る
YES
CMOSにPAPインストール・フラグを設定する
PAPチェックサムはOKか
NO
1
YES
PAPを求めるプロンプトを出す
EBDAにPWプロンプト・フラグを設定する
ユーザ入力をフェッチする
ユーザ入力=PAPか
NO
YES
移動検出フラグと第2の試行フラグをクリアする
CMOSにPAP入力フラグを設定する
戻る
移動がフラグ-1を検出
NO
YES
ユーザ入力=POPか
YES
NO
3回の試行か
NO
YES
第2の試行フラグを設定する
停止

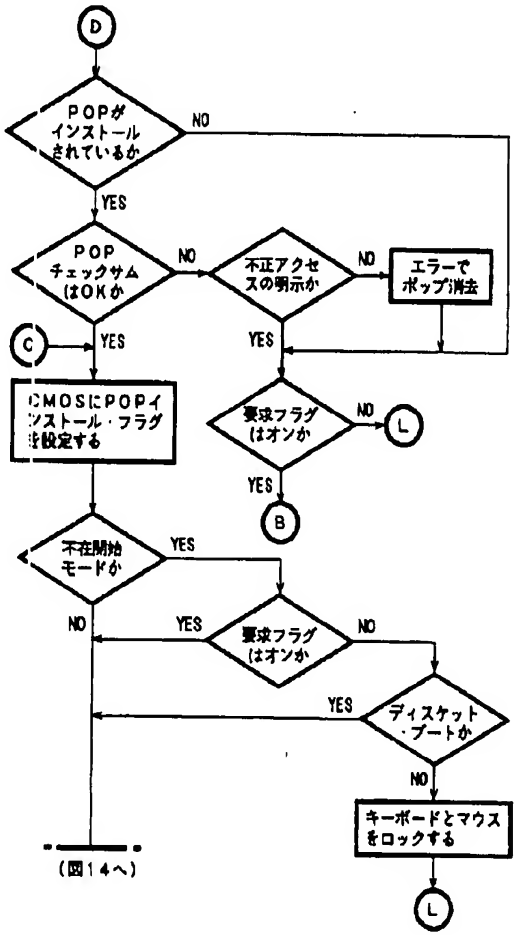
【図１１】


開始
要求フラグを保持し，ブート・フラグをクリアする
EEPROMがロックされているか
YES
NO
前にパスワードのプロンプトを出したか
YES
NO
ウォームブートか
YES
NO
CMOS内のフラグをクリアする
PAPがインストールされているか
NO
YES
CMOSにPAPインストール・フラグをセットする
PAPチェックサムはOKか
YES
NO
(図12へ)
エラーで停止
D
POPがインストールされているか
NO
YES
POPチェックサムはOKか
YES
C
NO
不正アクセス明示か
YES
NO
エラーでポップ消去
要求フラグはオンか
NO
P
YES
ブート・フラグを設定する
A

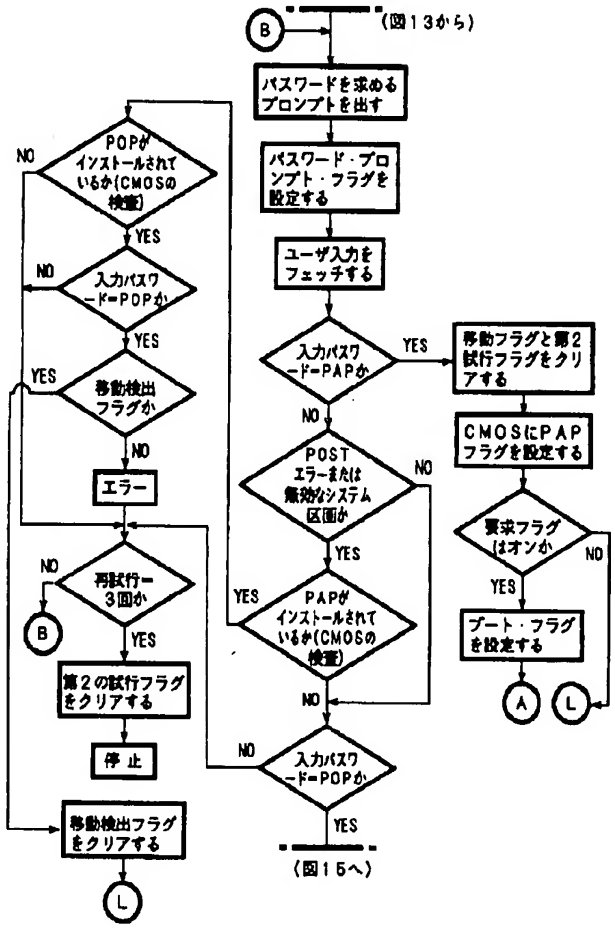
【図１２】


(図11から)
PAPがインストールされているか
NO
YES
PAPはコールド・スタートで入力されたか
NO
YES
要求フラグはオンか
YES
NO
EEPROM CRC，ブート・シーケンス，POPおよびCMOSのロックか
NO
YES
L
A
要求フラグはオンか
NO
YES
ブート・フラグを設定する
A
POPがインストールされているか
YES
L
NO
EEPROM CRC，ブート・シーケンス，PAPおよびCMOSのロックか
YES
NO
P

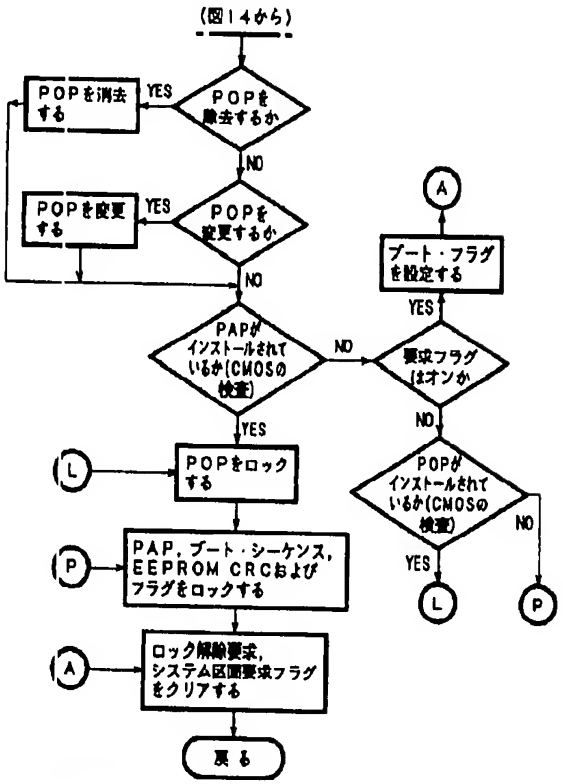
【図１３】


D
POPがインストールされているか
NO
YES
POPチェックサムはOKか
NO
不正アクセスの明示か
NO
エラーでポップ消去
C
YES
YES
CMOSにPOPインストール・フラグを設定する
要求フラグはオンか
NO
L
YES
B
不在開始モードか
YES
NO
YES
要求フラグはオンか
NO
YES
ディスケット・ブートか
NO
キーボードとマウスをロックする
L
（図１４へ）

【図１４】


B
（図１３から）
パスワードを求めるプロンプトを出す
パスワード・プロンプト・フラグを設定する
ユーザ入力をフェッチする
入力パスワード=PAPか
YES
移動フラグと第２試行フラグをクリアする
CMOSにPAPフラグを設定する
要求フラグはオンか
NO
YES
ブート・フラグを設定する
A
L
NO
POST エラーまたは無効なシステム区画か
NO
YES
PAPがインストールされているか(CMOSの検査)
YES
NO
入力パスワード=POPか
NO
YES
（図１５へ）
NO
POPがインストールされているか(CMOSの検査)
YES
NO
入力パスワード=POPか
YES
YES
移動検出フラグか
NO
エラー
NO
再試行=３回か
B
YES
第２の試行フラグをクリアする
停止
移動検出フラグをクリアする
L

【図１５】



フロントページの続き

(72)発明者　バルマー・イー・ニューマン
アメリカ合衆国フロリダ州ボカ・ラトン，
ダブリン・ドライブ7488番地